MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 37 | Issue 4 Article 10

2011

Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum

David Satola

Henry Judy

TOWARDS A DYNAMIC APPROACH TO ENHANCING INTERNATIONAL COOPERATION AND COLLABORATION IN CYBERSECURITY LEGAL FRAMEWORKS: REFLECTIONS ON THE PROCEEDINGS OF THE WORKSHOP ON CYBERSECURITY LEGAL ISSUES AT THE 2010 UNITED NATIONS INTERNET GOVERNANCE FORUM[†]

David Satola and Henry L. Judy[††]

† The content of this article is drawn in part from the proceedings of the Internet Governance Forum Workshop, Legal Aspects of Internet Governance: International Cooperation on Cyber-security, in Vilnius, Lithuania (Sept. 15, 2010), http://www.intgovforum.org/cms/component/chronocontact/?chronoformname=WSProposalsReports2010View&wspid=123, and the Background Paper prepared for the Workshop: Henry Judy, Jim Dempsey, David Satola, & Lee Hibbard, *Background Paper: Legal Aspects of Internet Governance: International Cooperation on Cyber-Security* (Sept. 3, 2010), http://www.afilias.info/webfm_send/135 [hereinafter Background Paper].

†† Henry L. Judy is Of Counsel at the international law firm K&L Gates LLP. David Satola is Senior Counsel in the Legal Vice Presidency at the World Bank. The authors are co-chairs of the Internet Governance Task Force of the Cyberspace Law Committee of the Section of Business Law of the American Bar Association. The views presented in this article are those of the authors in their individual capacities and do not necessarily reflect the views of the organizations with which they are associated or of any of the persons who participated as panelists in the Workshop or who participate in the organizations they represent. The authors would like to thank (i) Ali Zahid Ramin and Omar Martinez Sierra, both legal associates in the World Bank Legal Vice Presidency for early research on cybersecurity themes; (ii) Jim Dempsey of the Center for Democracy and Technology (CDT), Lee Hibbard of the Council of Europe, and Veni Markovski for their contributions to the Background Paper; and (iii) the participants of the Workshop (in order of appearance): Vinton Cerf, Vice President and Chief Internet Evangelist, Google, Inc., Ivalo Kalfin, Member of the European Parliament, Prof. Dr. Rolf H. Weber, University of Zürich, Alexander Seger, Head of Economic Crime, Council of Europe, Jayantha Fernando, Director of Legal Affairs, ICTA, Sri Lanka, Ericke Iriarte, Partner, Iriarte & Associates, Andrew McLaughlin, former Deputy U.S. Chief Technology Officer, Mike Silber, Member of the Board of Directors of ICANN, Bill Smith, Technology Evangelist, PayPal, Inc. and John Morris, General Counsel, CDT. The authors would also like to thank John D. Gregory of the Ministry of the Attorney General of Ontario, Canada, for his very helpful comments on a near final version of this article.

The focus of this article is on exploring the evolution of best practices for developing international cybersecurity legal frameworks. The article posits that due to the nature of the problems to be addressed, international legal responses to cybersecurity should be developed in an on-going process whereby

they are first deconstructed and approached in a modular fashion, and then integrated or re-integrated as consensus and political will develop. In a brief phrase, a dynamic "bottom up" approach should be used. Among the problems with taking a comprehensive approach (or "top down" approach) to cybersecurity legal frameworks is that the term "comprehensive" means all things to all people. The meaning varies depending on the physical, educational, and economic resources available in different jurisdictions. It differs depending on the sensitivity of the data to be protected and needs to reflect different cultural expectations and priorities, among many other factors. In addition, it must be recalled that the whole area of cybersecurity is both a relatively recent development as well as one that is notoriously in technological flux. While there is a continuing need for systematizing (and legal frameworks are simply a type of system), the very nature of cybersecurity resists systematizing or at least requires regular re-systematizing as the underlying reality alters with equal regularity.

Accordingly, while this article does not attempt to define "cybersecurity" as a unitary concept, it does propose a hopefully deeper understanding of the issues comprising cybersecurity through a modular approach. This article first looks at the landscape of the current causes of, and threats to, cybersecurity. In doing so, this article looks not only at what those threats are, but also looks at weaknesses "in the system" that may be exploited by, or that might exacerbate, those threats. This article then looks at the main component parts (modules) of cybersecurity (critical infrastructure protection, privacy, cybercrimes, institutional matters, etc.). It then looks at the current developments involving international responses and cooperative efforts with respect to each of the substantive areas (modules) and at recent attempts in the international sphere at addressing cybersecurity legal frameworks incorporating those developments. It concludes with some recommendations for a way forward.

I. CYBERSECURITY IS A GROWING CONCERN

In recent years, cybersecurity has become a major and expanding concern of governments and the private sector around the world. There has been a major shift in consciousness stemming from a variety of sources, including:

- Increased appreciation of how critical the Internet and its resources are in multiple spheres of human endeavor and how many infrastructures and systems are increasingly dependent on Internet connectivity and capacity;
- Continuing disclosures of major data breaches at financial institutions, other corporations, government agencies, and academic institutions globally;[1]
- Continuing releases of malware and the increased sophistication of those deployments;[2]
- Continuing reports of varying levels of governmental monitoring and filtering (or censorship) of Internet use and content;
- The cyber-attacks on key national infrastructure in Lithuania, Estonia, Georgia, and other countries and on the databases of major global business corporations;[3]
- Concerns with governmental and corporate espionage;
- Increased concern over cybercrime, including online fraud, identity theft, child pornography, theft of intellectual property, and related criminal money flows on the Internet; and
- Privacy concerns with corporate and governmental data access.

As the reach of the Internet continues to scale past a quarter of the world's population and given the apparent sporadic user awareness on implementation of security protocols, systems operating on the Internet are often perceived as soft targets to a range of persons and entities. These include criminal enterprises, "hackers" (whether for financial gain or as a challenge), cause-based groups, proxies for governments, and governments (including their military and intelligence agencies). Motives for

1. *See, e.g.*, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, FED. TRADE COMM'N (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm (describing settlement of data security breach by ChoicePoint); Eric Dash, *Data Breach Could Affect Millions of TJX Shoppers*, N.Y. TIMES, Jan. 19, 2007, http://www.nytimes.com/2007/01/19/business/19data.html (describing data breach at retailer T.J. Maxx).

2. Examples of malware include Confiker, Sutxnet, and the Zeus trojan.

3. The seriousness of this concern is highlighted by the report NATO 2020: ASSURED SECURITY; DYNAMIC ENGAGEMENT: ANALYSIS AND RECOMMENDATIONS OF THE GROUP OF EXPERTS ON A NEW STRATEGIC CONCEPT FOR NATO (2010), *available at* http://www.nato.int/strategic-concept/expertsreport.pdf. The report recommends changes in the NATO Strategic Concept to specify the characteristics of a cyber-attack that would trigger the obligation of collective response under Section 5 of the NATO treaty. *Id.*

the attacks range from financial gain to the advancement of national security interests, to the satisfaction of peer recognition, and to the advancement of various causes.[4]

Cybercrime and cyber-war have obvious direct negative effects on economic activity and, in fact, may intend such effects in the case of cyber-war. Cyber-defense can have similar direct negative effects, if only because of its high cost and the information inefficiencies due to deliberate isolation of networks and databases from one another. However, there are a number of situations in which information security has less obvious negative effects that reflect the tensions that are the subject of this article. For example, recent developments involving the BlackBerry service of Research in Motion (RIM) and demands by the United Arab Emirates (UAE), Saudi Arabia, and India have uncertain effects on the ability of businesses and various professionals to meet their legal obligations regarding trade secrets and confidential business information.[5] It has been recently reported that the UAE's Telecommunications Regulatory Authority has the key for BlackBerry services and can decrypt and monitor BlackBerry communications after obtaining a court order and that RIM has reached a similar agreement with authorities in India.[6]

In terms of an evolving cybersecurity legal framework, there are a number of evident vulnerabilities and impediments to effective international cooperation. Many of these were discussed in more depth at the Workshop.[7] Among these are:

4. The recent phenomenon of cause-based "leak sites," such as Wikileaks and Openleaks, adds a new dimension to these issues. *See Wikileaks*, N.Y. TIMES, http://topics.nytimes.com/top/reference/timestopics/organizations/w/wikileaks/index.html (last updated Apr. 25, 2011).

5. *See* Vikas Bajaj, *India May Soon Resolve BlackBerry Dispute*, N.Y. TIMES, Aug. 18, 2010, at B4, http://www.nytimes.com/2010/08/18/business/global/18rim.html?_r=1&ref=research-in-motion-ltd; Kevin J. O'Brien, *Saudis Relent a Bit on Shutting Down BlackBerry*, N.Y. TIMES, Aug. 10, 2010, at B2, http://www.nytimes.com/2010/08/11/technology/11rim.html?ref=research-in-motion-ltd.

6. *See SANS NewsBites: Dec. 14, 2010*, SANS, http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=98 (last visited Feb. 17, 2011); Adam Schreck, *UAE, BlackBerry Resolve Dispute, Averting Ban*, HUFFINGTON POST (Oct. 8, 2010, 10:58 AM), http://www.huffingtonpost.com/huff-wires/20101008/blackberry-crackdown.

7. *See* Internet Governance Forum Workshop, Legal Aspects of Internet Governance: International Cooperation on Cyber-security, in Vilnius, Lithuania (Sept. 15, 2010), http://www.intgovforum.org/cms/component/chronocontact/?chronoformname=WSProposalsReports2010View&wspid=123 [hereinafter Workshop].

- *Dissonance in national approaches to cybersecurity.* Different countries, even members of the same regional organizations, can take different approaches to the concept of cybersecurity in terms of national policies, laws, and implementation. Some countries see Internet governance as having state security at its core, by which they mean that the State can know exactly who sent and received every transmission, every transmission's traceroute, and the contents of every transmission; it can delete, block, and/or seize any transmission of which it disapproves; and it can punish efficiently those who send or receive unapproved transmissions. At the other end of the spectrum are countries and organizations that strongly believe that proper Internet governance, including Internet security, must be integrated and balanced with the type of freedoms protected by instruments such as the First, Fourth, Fifth, and Fourteenth Amendments of the United States Constitution, the European Union Charter of Fundamental Rights, and numerous United Nations human rights documents.[8] This "dissonance" can lead to a lack of effective coordination and can result in part because of a lack of multi-stakeholder participation in both policy-making and legislation.
- *Policy and implementation incoherence.* Even within countries there can be a disconnect between upstream policies promoting an "e"-agenda and the downstream protections of rights and property.
- *Outdated legal architecture that does not fit cyberspace well.* Cybersecurity is a twenty-first century problem that requires twenty-first century responses. However, in the legal sphere, many concepts developed in an analog era simply do not apply in a digital era or they cause friction when applied. For example, the lack of consensus on the fundamental and related issues of jurisdiction and sovereignty make it difficult to effectively cross borders to address international cybersecurity incidents.[9] A nation state may view its

8. *See generally* Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom at The Newseum (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm; Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Rights and Wrongs: Choices & Challenges in a Networked World at George Washington University (Feb. 15, 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm (discussing the importance of Internet freedom).

9. Jurisdiction is used in the sense of the legal capacity to make laws

sovereignty as being impaired if another nation state may exercise "jurisdiction" within its borders. However, nation states may view their sovereignty as being enhanced if by mutual agreement they obtain jurisdiction within each others' territories. In order for the rule of law to prevail, the inherent cross-border nature of cyberspace seems to require such agreements for the mutual expansion of jurisdiction.

- *Buggy code, bad practice.* Although it may be obvious, the fact that cybersecurity issues may arise from faulty (or "buggy") software code, simple human error, and sloppy behavior while using the Internet merits mentioning in this panoply of causes of cyber-insecurity.[10] Legal systems have not developed a consensus on addressing responsibility for offering such code in the marketplace. It is often left to contract law and, frequently, the software developer writes the exculpatory software license. However, if the licensee has sufficient market power, the licensor may be exposed to significant contractual and tort liabilities for defective code.
- *Existing tools and instruments are not fully applied or are only partially implemented.* Another source of vulnerabilities in the existing cybersecurity legal frameworks results from failure to apply the terms of existing instruments or only partial implementation of such instruments. Legal systems are increasingly responding to this source of vulnerability by establishing liability for failure to implement existing cybersecurity tools in a manner proportional to the sensitivity of the data held. This liability may be imposed because proportional security mechanisms were not employed as promised or regardless of whether a promise was made. However, this liability is often imposed on a case-by-case basis and not pursuant to statutory or regulatory requirements aimed at the particular issue.[11]

applicable to particular persons and events within a territory and to compel legal process and enforcement of laws with respect to such persons. Sovereignty is used in the broader sense of the total independent power of a nation state.

10. For a more thorough discussion of "buggy code" and the cybersecurity problems caused both by it and simple human error, see Andrew McLaughlin, Remarks at the International Cooperation on Cyber Security Workshop (Sept. 15, 2010), http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/661-123 [hereinafter Transcript].

11. *See, e.g.*, *In re* Dave & Busters, Inc., No. C-4291, 2010 WL 2453892 (F.T.C. May 20, 2010), *available at* http://www.ftc.gov/os/caselist/0823153

II. A MODULAR APPROACH TO THE MAIN THEMES OF CYBERSECURITY

The cybersecurity themes covered in this article are outlined below. This thematic analysis to cybersecurity allows and lends itself to a modular approach to the issues covered. As will be demonstrated in this article, there is good international practice in many of the themes covered, but there is no one-size-fits-all approach; every country addresses "cybersecurity" slightly differently. Deconstructing cybersecurity along these thematic, modular lines—rather than attempting to identify one all-encompassing, comprehensive model—also allows for greater selectivity when crafting the legislative responses to policy choices. In addition, disaggregating the issues that comprise cybersecurity lends itself to a better understanding of cybersecurity issues, and therefore to the ability to respond to them. In some cases this disaggregation is done in a layered fashion. In that vein, network security (the infrastructure layer) could be distinguished from both protocol security (the software layer) and from applications security (the applications layer). Cyber-threats can be in the form of cyber-attacks, but can also be the result of "mistakes" or even natural disasters. Similarly, responses can be viewed as preventative (*ex ante*) or loss-minimization (*ex post*). Even among *ex post* responses, there are at least two types: emergency fixes (loss prevention) and forensic analysis. New paradigms in international law such as shared responsibilities of states to ensure cybersecurity emerge from this analysis.

At the same time, it is important to recognize that a cybersecurity legal framework needs to have an internal logical consistency; the bits and pieces need to work together. The modular and layered approach allows national policy-makers and

/100608davebustersdo.pdf (ordering Respondent to establish and implement an information security program); *see also* FTC Agreement Containing Consent Order *In re* Twitter, Inc., No. 092-3093, 2010 WL 2638509, at *9 (F.T.C. June 24, 2010), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm (providing documents related to the FTC's complaint against Twitter for failure to safeguard consumer information); Marc S. Martin, Henry L. Judy & Lauren Bergen Pryor, *FTC Settles with Twitter—More Painful Lessons in Basic Data Security*, K&L GATES (July 1, 2010), http://www.klgates.com/newsstand/Detail.aspx?publication=6517; *Twitter Settles Charges that It Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program*, FED. TRADE COMM'N (June 24, 2010), http://www.ftc.gov/opa/2010/06/twitter.shtm.

legislators to tailor specific approaches to particular problems. It also allows policy-makers and legislators to prioritize matters that are most important to managing cybersecurity in their country.

In this section, we begin to explore the inter-relationships of these themes—for example, how security concerns play off of privacy concerns and vice versa; how crafting policy mandates certain inevitable trade-offs; how the manner in which these trade-offs are made by nation states results, in itself, in certain difficulties in enhancing international cooperation in forging consensus; and in the evolution of legal framework harmonization or inter-operability. Without casting judgment on these tradeoffs, it must at the same time be recognized by policy-makers, legislators, and regulators at the national level, and by stakeholders at the regional and international level, that certain balances must be obtained for the legal regimes to function.

The themes are:

1. *Security-Critical Infrastructure Protection*—this section will focus on securing the infrastructure over which data and communications flow.

2. *Digital Data Protection*—this section focuses on certain key substantive issues around protection of digital data and database management. This analysis is not focused exclusively on "privacy" issues; it also includes protection of confidential and proprietary data generally. Legal frameworks that enable persons to control the manner in which data about them is handled are clearly important from many points of view, including protection of human rights and the availability of concrete mechanisms to do so, such as Opt-in/Opt-out clauses and so-called "Breach Notification" requirements and requirements for data deletion and de-identification (anonymization). However, the ability of businesses and governments to function depends equally on the protection of confidential and proprietary data from inappropriate compromise.

3. Cybercrimes & Enforcement—the area of cybercrimes is perhaps one of the more clearly identified thematic areas and the one where there is almost universal agreement on best practice, as expressed in the Budapest Convention.[12]

12. *See* Council of Europe, Convention on Cybercrime, Nov. 11, 2001, E.T.S. No. 185 [hereinafter *Budapest Convention*], *available at* http://conventions.coe.int

4. Institutional Arrangements—finally, the article examines certain key institutional issues, mainly around critical infrastructure and data protection. This article does not address institutional issues regarding cybercrimes, for example, because these are mainly dealt with in the context of the police and jurisdiction of the criminal courts.

III. OVERVIEW OF CURRENT STATUS OF CYBERSECURITY THEMES

Section III undertakes a brief substantive overview of the major cybersecurity themes and surveys the institutions or organizations mainly responsibility for the evolution of international practice in those areas.

A. Security-Critical Infrastructure Protection

This section[13] deals with international legal aspects of critical infrastructure protection (CIP), in particular, protection of critical information infrastructure (CII).[14] CIP is one area where

/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=1&DF=01/09/2009&CL=ENG (last visited Mar. 6, 2011).

13. *See generally* David Satola & W.J. Luddy, Jr., *The Potential for an International Legal Approach to Critical Information Infrastructure Protection*, 47 JURIMETRICS J. 315 (2007), http://www.uncitral.org/pdf/english/colloquia/EC/Satola_LuddyArticleRev.pdf (reviewing global efforts to achieve cybersecurity). Certain parts of this section (III.A.1) are based on and drawn from Satola & Luddy.

14. For a working definition of these terms, see *id.*, at 316 n.1 ("'Critical Infrastructure' and 'Critical Infrastructure Protection' can be broadly defined."). As used in this article, "Critical Infrastructure" borrows from the definition found in *Commission Green Paper on European Programme for Critical Infrastructure Protection*, COM (2005) 576 final (Nov. 17, 2005) [hereinafter *Green Paper*], and as utilized in the Counsel Framework Decision 69/67, 2005 J.O. (L 225) [hereinafter *Council Decision*]. Namely, infrastructure (including physical resources, services, and information technology) is critical if the damage, destruction, or disruption of the infrastructure asset would have a negative and serious impact on security. *See Green Paper*, *supra*, at Annex 1. The *Green Paper* defines CII as "ICT systems that are critical infrastructures for themselves or that are essential for the operation of [other] critical infrastructures. . . ." *Id.* Of particular relevance to the "cyber" context is the definition of an "information system" used in the Council Decision: an "'information system' means any device or group of interconnected or related devises, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved, or transmitted by them for the purposes of their operation, use, protection, or maintenance." *See Council Decision*, *supra*, at article 1(a). The CRITICAL INFORMATION INFRASTRUCTURE HANDBOOK 26 (2006), defines "critical infrastructure" and "critical information infrastructure" as those assets which if

cooperation is more evident at some levels than others. This may be because there are a greater variety of actors in the space (from the governmental, non-governmental, academic, and private sectors) and it is an area that is thought of being more "technical" than "legal." As noted in the literature:

> "[B]est practice" regarding CIP is evolving, with interests of divergent stakeholders being served in different fora. For example, governments are interested in national security, the private sector and business communities are interested in secure transactions, consumers and users are interested in protecting personal data, and technologists and engineers are interested in the stability of the network.[15]

Much of CII, including the Internet, is owned and operated by the private sector; while other critical infrastructure is owned by governmental or quasi-governmental entities. "Open" networks and technologies have increased the interdependence of an increasingly wider range of stakeholders using the Internet and have threatened, or at least made more vulnerable, traditional constructs of the Westphalian "state" in attempting to isolate and deal with cybersecurity issues.[16]

1. International Cooperation

The private, governmental, and non-governmental sectors, on the basis of both national and international efforts, have been taking steps to increase the security of their products, services, and networks. These efforts include, for example, the work of international standards bodies, which range from the treaty-based International Telecommunication Union (ITU) to non-governmental but highly influential and essential bodies such as the Internet Engineering Task Force (IETF). Important issues for consideration include the role of standards and the role of government in developing standards. Internationally, a consensus appears to be emerging around both the process and substantive

"incapacitated or destroyed would have a debilitating impact on the national security and the economic and social welfare of a nation." The abbreviations "CIP" and "CIIP" are often used interchangeably because of the dependence of more physical critical infrastructure on secure and continuous information flows.

15. Satola & Luddy, *supra* note 13, at 317.

16. *Id.* at 318 ("This sector-specific, 'proprietary' approach in a world dominated by converged technologies is increasingly anachronistic.").

elements of CIP.[17] In terms of substantive elements, CIP is aimed at ensuring that disruptions to CII be brief, infrequent, isolated, and minimally detrimental.[18] This was highlighted by participants in the Workshop. Second, CIP should be dynamic and "process-oriented."[19] Although the rate of adoption has not been as rapid as one might ideally want, successful efforts by the Internet Corporation for Assigned Names and Numbers (ICANN) to promote development and adoption of security extensions for the domain name system (DNSSEC) illustrate how a private-sector led initiative (with government participation) can significantly enhance cybersecurity.[20]

Computer Emergency Response Teams (CERTs) are generally cooperative endeavors among governments, academic institutions, and commercial entities consisting mainly of technologists aimed at identifying cyber-vulnerabilities and defending against cyber-attacks.[21] Among other functions, they are intended to promote information sharing and better coordination among government

17. *Id.* at 318–19; *see also* ORG. FOR ECON. COOPERATION AND DEV., OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY (2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf; Creation of a Global Culture of Cyber Security, G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Jan. 31, 2003), *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf?OpenElement; Combating the Criminal Misuse of Information Technologies, G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Jan. 23, 2002), *available at* http://www.unodc.org/pdf/crime/a_res_56/121e.pdf; Combating the Criminal Misuse of Information Technologies, G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Jan. 22, 2001), *available at* http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

18. *See Green Paper*, *supra* note 14, at 1.

19. *See generally* Thomas J. Smedinghoff, *Where We're Headed: New Developments and Trends in the Law of Information Security*, 3 PRIVACY & DATA SECURITY L. J. 103 (2007) (discussing what is entailed in process-oriented approaches).

20. *See generally* DNSSEC: DNS SECURITY EXTENSIONS, http://www.dnssec.net (last updated Feb. 10, 2011) (providing information regarding the DNSSEC and its ties with ICANN); *see also* Press Release, Internet Corp. for Assigned Names & Numbers, Global Upgrade Makes Internet More Secure (July 28, 2010), *available at* http://www.prweb.com/releases/DNSSEC/Cyber_Crime/prweb4321774.htm (providing more information about DNSSEC); *see also generally* EUROPEAN NETWORK & INFO. SEC. AGENCY, GOOD PRACTICES GUIDE FOR DEPLOYING DNSSEC (2010), http://www.enisa.europa.eu/act/res/technologies/tech/gpgdnssec (describing role of DNSSEC and how to deploy DNSSEC).

21. Satola & Luddy, *supra* note 13, at 319. CERTs may also be referred to as Computer Security Incident Response Teams. *Cf. Incident Response Teams Around the World*, CERT, http://www.cert.org/csirts/csirt-map.html (last updated Mar. 5, 2008) (showing some of the CERT/CSIRT organizations throughout the world and noting how cooperation speeds response to attacks).

agencies and the private sector.[22] The Forum of Incident Response and Security Teams (FIRST) is an international non-governmental organization that seeks to promote global cooperation and coordination among these teams.[23] Its membership includes over 200 teams across 48 countries.[24] FIRST is an international organization bringing together a number of national CERTs.[25] It provides a forum for information sharing among CERTs and other incident response organizations and is also a repository of technical and other information about CIP.[26] As such, FIRST is an example of enhanced international cooperation in the area of cybersecurity.

The European Government CERTs (EGC) group has twelve member organizations.[27] The primary objective of EGC is to develop efficient and effective cooperation between the teams with a focus on incident and vulnerability management.[28] Primarily, EGC is an operational group with a technical focus; national policy is determined by other agencies within individual countries.[29]

CERTs typically focus on technical issues and their main function is information sharing providing primarily early warning functions.[30] In parallel, as the legal framework around CIP evolves, continued improvements in cooperation and consultation will be necessary in order to guard against differences in laws or the legal frameworks of countries resulting in divergences that would hinder rather than aid effective CIP. Different interest groups (stakeholders) need to talk to each other to ensure real and effective cybersecurity and to avoid a divergence in approach to CIP.[31] "As is already recognized by the literature, coordination, collaboration, and consultation are key."[32]

22. Satola & Luddy, *supra* note 13, at 328.
23. *See* FIRST, http://www.first.org (last visited Feb. 13, 2011).
24. *FIRST Members*, FIRST, http://www.first.org/members/map/ (last visited Feb. 13, 2011).
25. *See* FIRST, *supra* note 23.
26. *Id.*
27. EGC GROUP, http://www.egc-group.org (last visited Feb. 13, 2011) (describing EGC group and enumerating its member organizations).
28. *Facts (Part one)*, EGC GROUP, http://www.egc-group.org/facts1.html (last visited Feb. 13, 2011).
29. *Id.*
30. Satola & Luddy, *supra* note 13, at 320.
31. This phenomenon was noted with respect to cybercrime legislation by the European Union. *See Council Decision*, *supra* note 14, at L 69/68, ¶ 17.
32. Satola & Luddy, *supra* note 13, at 319.

As was pointed out in the Workshop, many countries have elements of the legal enabling environment addressing cybersecurity, but these national legal frameworks vary widely in terms of the manner in which cybersecurity issues are addressed. Moreover, even where countries do have specific provisions dealing with CIIP, differences exist between countries as to how CII is to be protected. The modules identified in Section II (CIP, digital data protection, cybercrimes, and institutional aspects) remain the focal points of evolving best practice.[33]

2. U.S. Private, Governmental, and Non-Governmental Cooperation

Perhaps the central lesson regarding CIP that emerged experimentally is that the effectiveness of any CIP program is directly proportional to the extent of cooperation among key private, governmental, and non-governmental actors. However, no general standards for such cooperation have emerged. Perhaps the most comprehensive and detailed instance of this form of cooperation is provided by the U.S. Comprehensive National Cybersecurity Initiative (CNCI).[34]

The CNCI began in 2008 under the Bush Administration when the President issued National Security Presidential Directive 54 (also known as "Homeland Security Presidential Directive 23") on January 8, 2008.[35] The directive called for the formation of the CNCI. The Bush administration developed CNCI to improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks and critical national infrastructure. Development of the CNCI continued under the Obama administration and on March 2, 2010, the White House published an unclassified summary of its CNCI, indicating

33. *Id.* at 321.

34. It should also be noted that 2010 saw a number of bills being introduced in the 111th U.S. Congress dealing with institutional issues, coordination of cybersecurity and protection of CII at the federal government level, as well as development of human capacity in the area of cybersecurity. *See, e.g.*, Protecting Cyberspace as a National Asset Act, S. 3480, 111th Cong. (2010), and Homeland Security Cyber and Physical Infrastructure Protection Act, H.R. 5548, 111th Cong. (2010). It could therefore be expected that the 112th Congress may take some legislative action in these areas.

35. The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Jan. 8, 2008). The full text of this Presidential Directive was never released to the public.

that it consisted of twelve "initiatives."[36] These included Initiative #2 to deploy an intrusion detection system of sensors across the Federal enterprise and Initiative #3 to pursue deployment of intrusion prevention systems across the Federal enterprise.[37]

To implement Initiatives #2 and #3, the U.S. federal government developed and deployed the Einstein Program (Einstein).[38] In general, Einstein is an intrusion detection system that monitors the Internet network gateways of government departments and agencies in the U.S. for unauthorized traffic and malicious content.[39] The original deployment was Einstein 1. The current deployment is Einstein 2, which conducts automatic full packet inspection of traffic entering or exiting U.S. government networks using signature-based intrusion detection technology.[40] Einstein 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity.[41]

Einstein 3 is currently being deployed on a limited pilot program basis and adds the additional capability to do real-time, full, deep-packet inspection and to respond appropriately to cyber-threats before harm is done, providing an intrusion prevention system supporting dynamic defense.[42] In addition, when deemed necessary by the Department of Homeland Security (DHS), Einstein 3 can send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA.[43] Einstein 2 is based on predefined attack signatures that come from internal, commercial, and public sources.[44] Under Einstein 3, DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and Department of Defense information assurance

36. *See The Comprehensive National Cybersecurity Initiative*, THE WHITE HOUSE, http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (last visited Feb. 13, 2011) [hereinafter *Comprehensive National Cybersecurity Initiative*].

37. *Id.* at 2–3.

38. *Id.*

39. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN 2, at 2–3 (May 19, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

40. *Id.* at 3–4.

41. *Id.* at 2.

42. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE, at 3 (Mar. 18, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

43. *Id.*

44. *Id.* at 7.

missions.[45] Intrusion detection systems require signatures of malicious traffic, allowing the system to search traffic flows for those malicious configurations. One advantage of Einstein 3 is that it connects to intelligence sources to provide a more complete list of signatures.[46]

Einstein 3 may also be deployed to monitor government computer traffic on private sector sites. Defense Department officials have suggested that Einstein 3 be used to provide CIP in the private sector, particularly with respect to CII, such as CII serving the financial, utility, and communication industries.[47]

The Einstein Program, and most particularly Einstein 3, has raised concerns among a number of privacy and civil liberties groups, particularly with the added capacity for deep-packet inspection, data sharing with NSA, and extension of the program to the private sector.[48]

In addition, concerns have been raised regarding a program called "Perfect Citizen" that is being implemented by Raytheon[49] under a $100 million classified contract with NSA. "Perfect Citizen" helps assess the vulnerabilities and capabilities of networks of domestic U.S. "critical infrastructure" such as utilities and nuclear power plants, both private and government run.[50] This is a response to increasing concern by intelligence officials about foreign surveillance of computer systems that control the electric grid and other U.S. infrastructure.[51] Google is partnering with NSA

45. *Id.* at 3.

46. *Id.*

47. *See* Kim Zetter, *Pentagon: Let Us Secure Your Network or Face the 'Wild Wild West' Internet Alone*, WIRED (May 27, 2010, 1:50 PM), http://www.wired.com/threatlevel/2010/05/einstein-on-private-networks; Kim Zetter, *U.S. Declassifies Part of Secret Cybersecurity Plan*, WIRED (Mar. 2, 2010, 4:19 PM), http://www.wired.com/threatlevel/2010/03/us-declassifies-part-of-secret-cybersecurity-plan.

48. *See* CTR. FOR DEMOCRACY & TECH., EINSTEIN INTRUSION DETECTION SYSTEM: QUESTIONS THAT SHOULD BE ADDRESSED 1 (July 2009), http://www.cdt.org/security/20090728_einstein_rpt.pdf; *see also generally* PRIVACY IMPACT ASSESSMENT FOR EINSTEIN 2, *supra* note 39 (explaining the privacy impact of Einstein 2); PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE, *supra* note 42 (explaining the privacy impact of the Initiative Three Exercise).

49. *See* OUR COMPANY, RAYTHEON, http://www.raytheon.com/ourcompany (last visited Apr. 15, 2011) ("[A] technology and innovation leader specializing in defense, homeland security and other government markets throughout the world.").

50. *See* Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J., July 8, 2010, http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

51. *Id.*

to help Google analyze the major corporate espionage attack that recently targeted its computer networks.[52]

The essential issue presented here is what the boundaries to cooperation are or what the boundaries to the *forms* of cooperation are. There is an obvious and difficult tension between the state's responsibility for public safety and the citizen's "right to be left alone" by the state. While these issues have been widely discussed and congressional hearings have been held, no consensus or resolution has emerged. The tension is an ancient one, but the resolution of the tension is far more difficult and consequential in the age of global cybersecurity. How these issues are being handled in the U.S. is but one example, albeit an illustrative one, of how the contours of the debate are taking shape. As suggested throughout this article, these issues continue to evolve rapidly and often unpredictably.

B. Digital Data Protection—Striking a Balance

A key area dealt with in cybersecurity legislation is the protection of digital data. This area may be thought of in terms of confidentiality of digital data generally and in terms of personal data more specifically. The more general term would include protection of trade secrets and other forms of intellectual property, protection of confidential client information, and protection of the sensitive or proprietary information of businesses and governments. The latter refers to information about particular human beings that may be identified or may be identifiable according to the standards of different jurisdictions. The latter is referred to by various terms, such as privacy, protection of private life, protection of personal information, and data protection. It also presents complex technical issues, such as the issue of attribution, the extent of the ability to determine the true senders of any message or request for information, and permissible means of indirect identification.[53] It appears that greater cross-border cooperation in the area of digital data protection could be

52. *See* Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, WASH. POST, Feb. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

53. This article focuses only on data in digital or electronic form. Nevertheless it is recognized that confidential and personal data is regularly held in hard copy form and that many of the considerations and legislative acts discussed apply equally to hard copy.

achieved. Though hard evidence is not available, the reasons hampering greater cooperation seem to revolve around issues of the balance and the trade-offs between data protection and security—issues that go to the core of the relationship between the individual and the state. This may make international cooperation more difficult.

1. Data Confidentiality

The protection of confidential digital data is critical to the functioning of global commerce and government on every level. It has been estimated that more than half of the value of U.S. businesses lies in their trade secrets and other intellectual property and that the value of such trade secrets and intellectual property lost each year is in the billions of dollars.[54] Private firms and other companies with fiduciary and near fiduciary obligations (law and accounting firms, for example) must be able to communicate confidentially. Even governments may have a need for confidential communications. The Wikileaks cases of 2010[55] have, ironically, laid bare both the sensitivities and the corresponding necessities regarding protecting data confidentiality in the Internet age.

It is a basic principle of knowledge management that appropriate sharing of information enables organizations to make smarter decisions and produce more successful results. Inappropriate sharing and inappropriate restrictions on sharing produces an increased risk to them of adverse consequences, including less intelligent decisions. While the various Wikileaks cases may have been aimed at uprooting the "conspiratorial nature" of governments,[56] they clearly demonstrate that organizations are information-gathering and information-processing machines and information is a tool that can be used to attack or to benefit. It remains to be seen what the effects of this type of use information will have on organizations in terms of their information gathering, dissemination, and, especially, information security processes and procedures. These incidents also highlight the difficult balancing issues of what sharing, restriction, and,

54. ENCYCLOPEDIA OF WHITE-COLLAR & CORPORATE CRIME 273 (Lawrence M. Salinger ed., 2005).

55. *See Wikileaks*, *supra* note 4 and accompanying text.

56. *See* Julian Assange, *State and Terrorist Conspiracies*, IQ (Nov. 10, 2006), http://iq.org/conspiracies.pdf.

therefore, security practices are appropriate for different types of organizations, different types of information, and, in different contexts, time. Thus, we see real examples of the benefits of looking at these cybersecurity questions in a more disaggregated and modular way.

2. Protection of Personally Identifiable Information (PII)

Treatment of PII is an essential part of creating a cybersecurity legal and regulatory enabling environment. The scope of the concerns that are inherently involved in the topic of PII protection is enormous—freedom of speech, freedom of expression, access to information, political speech, censorship, personal data collected for police or other surveillance purposes, Internet filtering, censorship, political speech online, and the treatment by third parties (data processors) of the collection, processing, and dissemination of data in digital format of an individual (data subject). Data subjects are real people and not juridical persons or other "constitutional" beings of privacy.

The trend globally in legal frameworks regarding PII protection has been towards the adoption of a "rights-based" or "constitutional" approach: balancing the "privacy" interests of the individual against security and other policy interests of the state, or against other interests, such as commercial confidentiality, that the state wishes to foster or avoid restricting. This constitutional approach is inherent in the European Directives and the Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Privacy Convention) (both discussed in more detail below)[57] Even India—which currently has only very limited legislation specifically dealing with PII protection—uses a constitutional approach to protecting privacy.[58] Much of available good international practices in terms

57. Council Directive 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:PDF; Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 [hereinafter Convention with Regard to Automatic Processing], *available at* http://conventions.coe.int/treaty/en/treaties/html/108.htm.

58. For a comprehensive discussion of the current state of Indian privacy protection, see SHRI RAHUL MATTHAN, APPROACH PAPER FOR A LEGISLATION ON PRIVACY (2010), *available at* http://persmin.gov.in/WriteReadData/RTI

of the treatment in legal frameworks of digital data are based in the constitutional approach to privacy.

There is a great deal in the media currently regarding privacy in the digital age. Indeed one outgrowth of the U.N.'s Internet Governance Forum (IGF) was the creation of a so-called Privacy Dynamic Coalition. Just prior to the IGF meeting in Sharm el Sheik in November 2009, the Coalition, along with civil society groups and other privacy experts, promulgated the so-called "Madrid Privacy Declaration,"[59] affirming privacy as a fundamental human right. While the Declaration takes a fairly wide sweep on privacy issues in the digital age, it also urges countries that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible. It also urges countries that have not already done so to adopt the CoE Privacy Convention. The Privacy Convention was opened for signature in 1981 and the CoE is currently involved in a consultation for the modernization of the Privacy Convention.

Among the key digital data issues dealt with from a cybersecurity point of view in this report are (1) protections against secondary use and (2) notification in the case of a breach of digital "privacy." A third area of digital data protection explored in the report, as will be seen from the country benchmarking section, is the variety of institutional forms that have been put in place in response to these digital data concerns.

Many countries have established data or privacy commissioners. International practice in this area, as with many others explored in this report, shows that there is no one-size-fits-all approach.

In this regard, for example, there is a major schism between the United States on the one hand and Europe (and other countries) on the other in terms of the structure of privacy and the regulation of how data is gathered and used. To generalize considerably, in the United States, privacy law is applied differentially depending on the economic or business sector and on the type of personal data. For example, different laws are applied to personal data held by financial institutions, educational

/aproach_paper.pdf.

59. *Madrid Privacy Declaration*, THE PUBLIC VOICE (Nov. 3, 2009), http://thepublicvoice.org/madrid-declaration.

institutions and health care providers and to drivers license data, video rental data, etc. In Europe, personal data is regulated in general terms regardless of these distinctions pursuant to European Union (E.U.)-wide Directives.[60] U.S. law in general tends to be more permissive about the level and timing of the consent of the data subject that needs to be given about the personal data that may be collected and shared. The law in Europe and in countries following the European model tends to be less permissive in that regard. To bridge this gap, the U.S. Department of Commerce and the European Commission have developed a "safe harbor" framework of data protection principles.[61] This safe harbor is designed to provide U.S. organizations with a means to satisfy the European Union's legal requirement that "adequate" data protections be afforded to personally identifiable information transferred from the European Union to the United States, since U.S. law is not considered to be adequate in that regard.

Regardless of the differences in systems and approaches, certain principles can be distilled from the variegated practices. In terms of managing one's own data, a data subject should be enabled through the legal framework to be able to verify the data about himself or herself and make such corrections as are necessary in a timely and transparent fashion. In the words of one scholar, a data subject should not be "excluded" from his or her own data.[62]

Data breach notification is another area of concern to data subjects, policymakers, and regulators around the world, and—again—practice is varied. Even in the E.U. (under the umbrella of a common framework Directive) there are a variety of approaches to data breach notification. First, there must be a determination of the nature of the data that is subject to protection. This depends on how "personal data" is defined in the law. Then a

60. *See* Council Directive 95/46, *supra* note 57 (discussing the protection of individuals with regard to the processing of personal data and on the free movement of such data); Council Directive 02/58, Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37–47 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF (concerning the processing of personal data and the protection of privacy in the electronic communications sector).

61. *See generally Safe Harbor*, EXPORT.GOV, http://www.export.gov/safeharbor (last updated Mar. 31, 2011) (providing the background and links to the Safe Harbor frameworks).

62. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 134–35 (2008).

determination needs to be made as to what information about the person is covered and what exceptions, if any, exist. For example, "public" information would probably not be covered, but that depends on how "public" is defined. Next is a determination of what constitutes a "trigger" for a breach notification—how is it determined when data about a person has been acquired by a third party in an unauthorized fashion under the law, and are there any exceptions, such as for encrypted or redacted data? If a notice obligation applies, to whom does the notice of breach go—to the data subject, to the data intermediary, to the public authorities, or some combination? At what time must the notice be given, in what form, and how much detail about the breach must be included in the notice? Finally, what are the remedies to be provided and how and by whom are they enforced?

A number of info-security standards are being developed that may apply here as well. These include the practices of the bank and credit card industries and even the International Standards Organization (ISO), ISO 17799, for example.[63]

3. Developments in the E.U. and the U.S.

In the E.U., the principal framework for the protection of PII is the E.U.'s Data Protection Directive 95/46/EC (E.U. Directive).[64] The E.U. Directive regulates secondary use of data, requiring that data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[65] One of the main purposes of the E.U. Directive was to achieve harmonization across the E.U. Article 29, setting up a "Working Party on the Protection of Individuals with Regard to the Processing of Personal Data," that provides advice concerning the meaning and application of the E.U. Directive including whether Member States are compliant with the Directive.

The European Commission conducted a public consultation in 2009 on "the current legal framework" for the fundamental right to protection of personal data.[66] The subsequent report stated: "The

63. *See* INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, http://www.iso.org/iso/home.html (last visited Mar. 15, 2011).

64. *See* Council Directive 95/46, *supra* note 57.

65. *Id.* art. 6, § 1(b).

66. FRANCIS ALDHOUSE, INFO. POL'Y & RTS., EUROPEAN COMMISSION REVIEW OF DIRECTIVE 95/46/EC: PRIORITY POINTS FOR CHANGE, § 1.1, n.1 (2009), *available at* http://ec.europa.eu/justice/news/consulting_public/0003/contributions/citizens

Directive was developed at a time before the full commercialisation [sic] of the internet and when many of the technologies underlying much modern data processing were still experimental."[67] The report went further and concluded that these changes did not result in any need to address the underlying fundamental principles of data protection, including the principles found in the OECD Guidelines of 1980,[68] but recognized that certain elements of the E.U. Directive could be updated to simplify processes and adjust "the legal framework to take account of changes in the handling of personal information brought about by fifteen years of technological change."[69]

As a result of this consultation, the E.U. Commission issued a Communication to the E.U. Parliament and the Council on November 4, 2010 subtitled "A comprehensive approach on personal data protection in the European Union" (E.U. Communication).[70] The E.U. Communication proposed a wide-ranging and fundamental update of E.U. data protection law. Less than a month later, on December 1, 2010, the U.S. Federal Trade Commission (FTC) released a preliminary staff report entitled "Protecting Consumer Privacy in an Era of Rapid Change" (FTC Proposal).[71] The FTC Proposal sets forth a broad new framework, which like the E.U. Communication, suggests wide-ranging and fundamental revisions to U.S. privacy law. A major Internet privacy report was issued by the U.S. Department of Commerce's Internet Policy Task Force on December 16, 2010. The report is entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." This report, along with the FTC Proposal, will inform policy decisions by a recently created White House Privacy and Internet Policy Subcommittee. This Subcommittee is expected to address and coordinate the direction

/aldhouse_francis_en.pdf.

67. *Id.* § 2.1.

68. *See infra* Part III.B.6.

69. FRANCIS ALDHOUSE, *supra* note 66, at § 4.3.

70. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 2, COM (2010) 609 final (Nov. 4, 2010) [hereinafter *E.U. Communication*], *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

71. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010) [hereinafter FTC PROPOSAL], *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf.

of U.S. federal law on privacy regulation from the standpoint of the Executive Branch.[72]

Although there are a number of differences between the FTC Proposal, the Department of Commerce report, and the E.U. Communication, their commonalities are notable, including an emphasis on prior consent, stronger remedies for violations of privacy, and the role of changes in technology in driving the need for changes in privacy law. Both focused strongly on the role of "profiling," that is, the use of technologies for data gathering and analysis and related business and governmental practices that enable the creation of "profiles" that have the same effects, for all practical purposes, as gathering obviously personal information.[73] The E.U. Communication also focused on the effects of cloud computing on privacy law.[74] On December 15, 2010, the European Parliament approved a strong and comprehensive resolution asking the E.U. Commission to carry out an in-depth study of "new advertising practices," including behavioral advertising.[75]

A principal factor in driving this tendency toward increasing convergence in the U.S. and E.U. legal regimes for data protection is the high level of integration of the U.S. and E.U. economies, as reflected in the number of corporate offices in each other's jurisdictions and the significant personal data flows between the two economies.

This convergence is further advanced by the adoption on July 6, 2010 of Mexico's "Law on the Protection of Personal Data Held by Private Parties."[76] In many ways, this law is more robust than

72. U.S. DEP'T OF COMMERCE, INTERNET POL'Y TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK, http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf; "*Do-Not-Track" Legislation: Hearing Before the Subcomm. on Commerce, Trade and Consumer Prot. of the H. Comm. on Energy and Commerce*, 111th Cong. 9 (2010) (statement of Daniel J. Weitzner, Associate Administrator for Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of Commerce).

73. *E.U. Communication*, *supra* note 70, at § 2.2.4; FTC PROPOSAL, *supra* note 71, at 37.

74. *E.U. Communication*, *supra* note 70, at § 2.2.3.

75. Resolution on the Impact of Advertising on Consumer Behaviour, EUR. PARL. DOC. T7-0484/2010 (Dec. 15, 2010), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0484&language=EN.

76. The official Spanish language version of the law is available at http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010; an unofficial English language translation is available courtesy of the International Association of Privacy Professionals at https://www.privacyassociation.org/images

approaches taken to data protection in the United States, and, depending on forthcoming implementing regulations, it may bring Mexican privacy law far closer to, or go beyond, the approaches of the E.U. Directive.

4. CoE Privacy Convention

The CoE Privacy Convention is the only international treaty dealing specifically with data protection. It is mainly a European instrument, although it is open to signature by countries outside of Europe. One key feature of the convention is that it is not self-executing, so its adherents would need to incorporate its principles into national legislation. For example, similarly to the E.U. Directive, the CoE Privacy Convention requires that data be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes."[77] On the specific subject of profiling, the CoE Committee of Ministers recommended to all member states that profiling be permitted, subject to certain exceptions, only if "the data subject or her or his legal representative has given her or his free, specific and informed consent."[78]

5. Asia-Pacific Economic Cooperation

Asia-Pacific Economic Cooperation (APEC) is a forum that was established in 1989 for twenty-one Pacific Rim countries and that seeks to promote free trade and economic cooperation throughout the Asia-Pacific region.[79] They are referred to as "Member Economies." The population of APEC's Member Economies exceeds 2.7 billion people, and the Member Economies represent approximately fifty-four percent of world real GDP and forty-four percent of world trade.[80] APEC's activities are focused on three key

/uploads/Mexico%20Federal%20Data%20Protection%20Act%20(July%202010).pdf.

77. *See* Convention with Regard to Automatic Processing, *supra* note 57, art. 5b.

78. Comm. of Ministers, *Recommendation of the Comm. of Ministers to Member States on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling*, 1099th Meeting, Doc. No. CM/Rec (2010)13, § 3.4(b) (2010), *available at* https://wcd.coe.int/wcd/ViewDoc.jsp?id=1710949&Site=CM.

79. *See* ASIA-PACIFIC ECON. COOPERATION, http://www.apec.org (last visited Mar. 6, 2011).

80. *See* ASIA-PACIFIC ECON. COOPERATION, APEC AT A GLANCE: ADVANCING FREE TRADE FOR ASIA-PACIFIC PROSPERITY 2 (2010), *available at* http://publications.apec.org /publication-detail.php?pub_id=1077 (click "Download Document" on the right

areas: trade and investment liberalization, business facilitation, and economic and technical cooperation. In support of these goals, APEC has established the APEC Privacy Framework (Framework).[81] Although the Framework speaks to privacy regulation within Member Economies, its focus is on information sharing between economies, cooperatively developing a system of cross-border privacy rules for use by businesses, and developing arrangements for cross-border cooperation in investigation and enforcement. The Framework addresses privacy as a consumer protection and trust issue rather than from the standpoint of human rights and civil liberties and it places heavy reliance on self-regulation.

Recently APEC established a Cross-Border Privacy Enforcement Arrangement (CPEA) that facilitates information sharing and cooperation among authorities responsible for data and consumer protection in the APEC region.[82] The CPEA was endorsed by APEC Ministers in November 2009 and commenced operation on July 16, 2010. The initial signatories, that is, participating privacy enforcement authorities, were the Privacy Commissioners from Australia, New Zealand, Canada, Hong Kong, and the U.S. Federal Trade Commission.[83]

Many privacy advocates do not regard the Framework, the CPEA and APEC's other privacy oriented projects as providing an appropriate level of protection, especially with respect to the most recent technological challenges. However, it is also generally recognized that APEC's initiatives represent significant forward steps in privacy protection, particularly in a number of the less developed countries in the region, and may constitute valuable building blocks for further evolution of this legal framework.

side of the webpage).

81. ASIA-PACIFIC ECON. COOPERATION, PRIVACY FRAMEWORK (2005), *available at* http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

82. ASIA-PACIFIC ECON. COOPERATION, APEC COOPERATION ARRANGEMENT FOR CROSS-BORDER PRIVACY ENFORCEMENT 1–2 (2010), *available at* http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf; *see also* ASIA-PACIFIC ECON. COOPERATION, APEC FACT SHEET—APEC CROSS-BORDER PRIVACY ENFORCEMENT ARRANGEMENT (2010), *available at* http://www.apec.org/About-Us/About-APEC/Fact-Sheets/Collection/~/media/Files/AboutUs/Factsheet/FS_CPEA_020710.ashx (providing more information on the Cross-Border Privacy Enforcement Arrangement).

83. *See FTC Joins New Asia-Pacific Multinational Network of Privacy Enforcement Authorities*, FED. TRADE COMM'N (July 19, 2010), http://www.ftc.gov/opa/2010/07/apec.shtm.

6. Other International Sources

Another source of data protection principles is the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (Guidelines).[84] The Guidelines are built around eight principles for treatment of personal data: collection (limiting the means by which data are collected), data quality (dealing with the relevance of the data collected), "purpose specification" (requiring that the purposes for which data are collected are known in advance and subsequent use is limited to those purposes), use limitation (limiting disclosure of data), safeguards (protecting data against risk of loss or unauthorized access), openness (relating to the operational standards of the data controller), individual participation (setting forth the rights of the "data subject" over his or her own data), and accountability (imposed on data controllers).[85] The Guidelines form the basis of the legislative framework in Canada, for example.

Finally, it is important to note that at the two most recent meetings of the International Conference of Data Protection and Privacy Commissioners, the Conference has adopted resolutions with respect to the adoption of binding global privacy standards and facilitating cross-border enforcement actions. Perhaps the most comprehensive and substantive of these resolutions is the so-called "Madrid Resolution," adopted in November 2009.[86]

C. Cybercrime—The Law Enforcement Response

International best practice, if not international cooperation and collaboration, is more evident in the area of cybercrime, perhaps due in part to the near universality of the substantive provisions of the Budapest Convention (defined below).

84. *See* ORGANISATION FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited Mar. 6, 2011).

85. *See id.* at pt. 2.

86. *See* INT'L CONFERENCE ON DATA PROT. AND PRIVACY COMM'RS, INTERNATIONAL STANDARDS ON THE PROTECTION OF PERSONAL DATA AND PRIVACY: THE MADRID RESOLUTION (2009), *available at* http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

1. International Experience

At the recent twelfth pentennial U.N. Crime Congress, held in April 2010 in Salvador, Brazil, efforts to negotiate a global cybercrime treaty were unsuccessful despite intense discussion among the parties.[87] A number of major powers disagreed over national sovereignty issues and concerns for human rights. For example, the Budapest Convention permits police under certain circumstances to cross national boundaries to access servers without consent from local authorities. Russia, for example, asserted that permitting foreign law enforcement agencies to conduct Internet searches inside Russian borders violated the Russian Constitution. In addition, because of phenomena such as cloud computing, which can result in data being transferred across national boundaries to servers in any location, police from one country can be denied access to data in a foreign location. Other countries insisted on the need for privacy provisions that would protect users' data from police investigation when it is stored in another country via a cloud computing partner.

These and other issues present countries with inherently conflicting policy objectives and cultural clashes, including the need to balance different interests and rights such as security and privacy, and are compounded by the impact of rapidly developing technologies on the structure of any agreement. The resolution of issues on this level suggests the need for the kind of bottom-up approach suggested by this article.

a. Council of Europe

In the area of cybercrime, the 2001 Convention of the Council of Europe ("CoE Convention" or the "Budapest Convention")[88] is a historic milestone vis-à-vis cybersecurity and cybercrime and provides a nearly universal standard of good international practice regarding legal frameworks for the protection against "cybercrimes." Although the Convention was promulgated under the auspices of the Council of Europe, it is open to signature by any country. In fact, a number of non-CoE countries (for example, the United States) have not only signed but also ratified the

87. *See The Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, UNITED NATIONS OFFICE ON DRUGS & CRIME, http://www.unodc.org/unodc/en/crime-congress/12th-crime-congress.html (last visited Mar. 6, 2011).

88. *Budapest Convention*, *supra* note 12.

Convention.

The Convention addresses three sets of issues: the categories of cybercrime that nations should address in their criminal codes, the authorities governments should adopt in order to access communications or stored records for evidentiary purposes, and mechanisms for transnational cooperation. So far, the Budapest Convention has entered into force in thirty countries, and another twenty-one countries have signed it or been invited to accede. Moreover, according to the CoE, some one hundred countries have made use of the Budapest Convention when developing national cybercrime legislation.

Cybercrime raises many traditional law enforcement issues. A recent dispute between the U.S. and the U.K., for example, illustrates how traditional tensions over extradition also arise in the cybercrime context.[89] While local limitations of resources and expertise present hurdles to effective law enforcement, one of the transnational barriers of a legal nature that should be considered is the existence of nation states that serve as "safe havens" and what dynamics and incentives are involved for a nation state to maintain "safe haven status."

The Convention consists of four chapters[90]:

- **Chapter I**, titled *Use of terms*, includes definitions of "computer system," "computer data," "service provider," and "traffic data."
- **Chapter II**, titled *Measures to be taken at the national level*, consists of three sections: *Substantive criminal law* (Section 1), *Procedural law* (Section 2), and *Jurisdiction* (Section 3). All sections in the Convention are further subdivided into "Titles." The section on substantive criminal law is divided into five titles with the first four titles classifying different types of offenses:
  - *Offences* [sic] *against the confidentiality, integrity and availability of computer data and systems*, which include offenses such as illegal access, illegal interception, data interference, system interference, and misuse of devices.
  - *Computer related offences* [sic], which include forgery and fraud.

89. *See* Jo Adetunji & Matthew Weaver, *Gary McKinnon May Avoid US Extradition, David Cameron Suggests*, THE GUARDIAN, July 21, 2010, http://www.guardian.co.uk/world/2010/jul/21/gary-mckinnon-extradition-david-cameron.

90. *Budapest Convention*, *supra* note 12, passim.

  - *Content-related offences* [sic], which include offences related to child pornography.
  - *Offences* [sic] *related to infringements of copyright and related rights.*
- The section on procedural law includes *Common provisions* (Title 1) that apply to the Convention's articles on substantive criminal law, "other criminal offences [sic] committed by means of a computer system," and to "the collection of evidence in electronic form" relating to criminal offences [sic]. There is also a title on *Expedited preservation of stored computer data* and includes provisions dealing with *Production order*, *Search and seizure of stored computer data*, *Real-time collection of traffic data*, and *Interception of content data.*
- **Chapter III** on *International co-operation* includes general principles relating to "international cooperation," "extradition," "mutual assistance," and "spontaneous information." The chapter also contains procedures pertaining to *Requests for mutual assistance in the absence of applicable international agreements* and to *Confidentiality and limitation on use* including *Specific Provisions* (Section 2) on *Mutual assistance regarding provisional measures* (Title 1), *Mutual assistance regarding investigative powers* (Title 2), and on a *24/7 Network.*
- **Chapter IV** titled *Final provisions* contains standard provisions found commonly in Council of Europe treaties. Importantly, in accordance with Article 40, any state may "declare that it avails itself of the possibility of requiring additional elements" as provided for under certain articles.

In accordance with Article 42, any state may "declare that it avails itself of the reservation(s) provided for" in certain articles. By ratifying or acceding to the Convention, countries agree to ensure that their domestic laws criminalize the conduct described in the section on substantive criminal law and establish the procedural tools necessary to investigate and prosecute such crimes.

The Convention uses technology-neutral language, so that it applies to and covers both current and future technologies. States may exclude petty or insignificant misconduct from the offenses it defines. Offenses must be committed intentionally for criminal liability to arise. Additional specific intentional elements only apply to certain offenses—for instance, to computer-related fraud,

with the requirement of fraudulent or dishonest intent of procuring economic benefit.

International coordination and cooperation are necessary for the prosecution of cybercrime and other information security and network security issues and governments must take innovative steps to curb these serious threats. Offenses must be committed "without right," referring to conduct undertaken without authority or conduct not covered by established legal defenses, excuses, justifications, or relevant principles under domestic law. These definitions are not intended to criminalize legitimate and common activities inherent in the design of systems and networks or legitimate operating or commercial practices.

b. International Telecommunications Union (ITU)

There are many resources interpreting and summarizing the Convention. In addition, at the international level, the ITU has taken a leading role in collecting and synthesizing experience regarding cybercrime legislation in its Guide and Toolkit.[91]

The ITU in conjunction with other partners took the leading role in organizing the World Summit on the Information Society (WSIS),[92] which was held in two phases: in Geneva in 2003 and Tunis in 2005. Governments, policy-makers, and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with the development of a global information society, including the development of compatible standards and laws.

91. *See* INT'L TELECOMM. UNION, CYBERSECURITY GUIDE FOR DEVELOPING COUNTRIES (2007), *available at* http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf.

92. *See generally* WORLD SUMMIT ON THE INFORMATION SOCIETY, http://www.itu.int/wsis/index.html (last visited Mar. 15, 2011) (providing links and information on the WSIS).

The outputs of the Summit are contained in the *Geneva Declaration of Principles*,[93] the *Geneva Plan of Action*,[94] the *Tunis Commitment*,[95] and the *Tunis Agenda for the Information Society*.[96] Under the *Tunis Agenda for the Information Society*, the ITU was entrusted to take the lead as the sole facilitator for WSIS Action Line B5: "Building confidence and security in the use of ICTs [information and communication technologies]."[97] The ITU Secretary General launched the Global Cybersecurity Agenda (GCA) in May 2007 as a global framework for dialogue and international cooperation aimed at proposing strategies to enhance security in the Information Society.

c. The Commonwealth

In an effort to harmonize computer-related criminal law in the Commonwealth countries,[98] experts gathered to present a model law at the Commonwealth Conference of Ministers in 2002. Importantly, the model law, titled the Computer and Computer Related Crimes Bill,[99] shares the same framework as the Convention to limit conflicting guidance. It serves as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries.

93. *See* World Summit on the Info. Soc'y, *Declaration of Principles*, Doc. No. WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003) [hereinafter Geneva Declaration of Principles], *available at* http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

94. *See* World Summit on the Info. Soc'y, *Plan of Action*, Doc. No. WSIS-03/GENEVA/DOC/5-E (Dec. 12, 2003), *available at* http://www.itu.int/wsis/docs/geneva/official/poa.html.

95. *See* World Summit on the Info. Soc'y, *Tunis Commitment*, Doc. No. WSIS-05/TUNIS/DOC/7-E (Nov. 18, 2005), *available at* http://www.itu.int/wsis/docs2/tunis/off/7.html.

96. *See* World Summit on the Info. Soc'y, *Tunis Agenda for the Information Society*, Doc. No. WSIS-05/TUNIS/DOC/6(Rev. 1)-E (Nov. 18, 2005), *available at* http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

97. Geneva Declaration of Principles, *supra* note 93, at 5.

98. *See generally* COMMONWEALTH SECRETARIAT, http://www.thecommonwealth.org (last visited Feb. 10, 2011) (providing information on the Commonwealth, including a list of the member states).

99. COMMONWEALTH SECRETARIAT, MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME (2002), *available at* http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

A later Meeting of Senior Officials of Commonwealth Law Ministers was held in October 2007 to address laws to combat terrorism and money-laundering, which included discussion on cybersecurity and cybercrime.

d. The United Nations Convention Against Transnational Organized Crime (CTOC)

The CTOC was adopted by General Assembly Resolution 55/25 on November 15, 2000 and it came into force on September 29, 2003.[100] It is the main international instrument in the fight against transnational organized crime and seeks to promote international cooperation to prevent and combat transnational organized crime more effectively. Here, it merits noting that the CoE Convention is aimed principally at strengthening internal law regarding cybercrimes, while the CTOC Conventions is aimed generally at cross border criminal activity.

Although the CTOC Convention does not provide a single, agreed upon definition of organized crime per se, its provisions do provide elements of a concept of organized crime. For instance:

- An organized criminal group is defined as three or more persons working together to commit one or more serious crimes in order to obtain financial or other material benefit.
- Transnational crimes are defined as:
  - offenses committed in more than one State;
  - offenses committed in one State, but a substantial part of preparation, planning, direction, or control takes place in another;
  - offenses committed in one State, but involving an organized criminal group that engages in criminal activities in more than one State; and
  - offenses committed in one State, but having substantial effects in another State.
- Serious crime is defined as conduct constituting an offense punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

100. *See United Nations Convention Against Transnational Organized Crime and Its Protocols*, UNITED NATIONS OFFICE ON DRUGS & CRIME, http://www.unodc.org/unodc/en/treaties/CTOC/index.html (last visited Feb. 11, 2011).

e. United Nations System Decisions, Resolutions, and Recommendations

Some additional relevant United Nations system decisions, resolutions, and recommendations include[101]:

- The United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ)[102] 2007—Resolution 16/2 of April 2007 on *Effective crime prevention and criminal justice responses to combat sexual exploitation of children* (notably, paragraphs 7 and 16).
- The United Nations Economic and Social Council (ECOSOC)[103] Resolution E/2007/20 of July 26, 2007 on *International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime (E/2007/30 and E/2007 SR. 45).*
- ECOSOC Resolution 2004/26 of July 21, 2004 on *International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.*
- The *Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century* (paragraph 18), endorsed by General Assembly Resolution 55/59 on December 4, 2000, and paragraph 36 of *Plan of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first century* annexed to, and noted by, General Assembly Resolution 56/261 of January 31, 2002.
- The Bangkok Declaration on *Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice* (paragraphs 15 and 16), endorsed by General Assembly Resolution 60/177 of December 16, 2005.
- Recommendations of an ad hoc Congress Workshop on *Measures to Combat Computer-Related Crime.* Paragraph 2 of General Assembly Resolution 60/177 invited governments to implement all the recommendations adopted by the Eleventh Congress.

101. This list is non-exhaustive.

102. *See The Commission on Crime Prevention and Criminal Justice*, UNITED NATIONS OFFICE ON DRUGS & CRIME, http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html (last visited Mar. 15, 2011).

103. *See* UNITED NATIONS ECONOMIC & SOCIAL COUNCIL, http://www.un.org/ecosoc (last visited Feb. 11, 2011).

- General Assembly Resolutions 55/63 of December 4, 2000 and 56/121 of December 19, 2001 on *Combating the criminal misuse of information technologies.* This latter resolution invites Member States, when developing national law, policy, and practice, to combat the criminal misuse of information technologies and to take into account, inter alia, the work and achievements of the CCPCJ.
- Various resolutions by the Commission on Narcotic Drugs,[104] including Resolution 48/5[105] on *Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime* and Commission on Narcotic Drugs Resolution 43/8[106] of 15 March 2000 on the Internet. ECOSOC Resolution 2004/42 also addresses the *Sale of internationally controlled illicit drugs to individuals via the Internet.*
- Paragraph 17 of the General Assembly Resolution 60/178 of December 16, 2005 on *International cooperation against the world drug problem.*
- ECOSOC Resolution 2004/42 on the *Sale of internationally controlled illicit drugs to individuals via the Internet.*

Subsidiary bodies of the Commission on Narcotic Drugs (e.g., the Sub-commission on Illicit Drug Traffic and Related Matters in the Near and Middle-East and regional Heads of National Drug Law Enforcement Agencies (HONLEA) meetings) have also published relevant conclusions and recommendations. Additionally, the International Narcotics Control Board (INCB) published recommendations in its annual report for 2005 to curb the spread of illicit sales of controlled substances over the Internet, particularly pharmaceutical preparations.

104. *See The Commission on Narcotic Drugs*, UNITED NATIONS OFFICE ON DRUGS & CRIME, http://www.unodc.org/unodc/en/commissions/CND/index.html (last visited Mar. 15, 2011).

105. *See* E.S.C. Res. 48/5 (2005), *available at* http://www.unodc.org/pdf/resolutions/cnd_2005_48-5.pdf.

106. *See* E.S.C. Res. 43/8 (Mar. 15, 2000), *available at* http://www.unodc.org/documents/commissions/CND-Res-2000-until-present/CND-2000-Session43/CND-Resolution-43-08.pdf.

2. Other Regional Experience

Regional experience can also inform the debate. In that regard, several regional sources are highlighted here.

a. The League of Arab States

Several countries in Southwest Asia and North and Northeast Africa comprising the League of Arab States (Arab League)[107] have adopted cybercrime legislation, such as Tunisia,[108] Saudi Arabia,[109] and the United Arab Emirates (UAE).[110]

From a regional perspective, the recently concluded *International Telecommunication Union Regional Cybersecurity Forum for Africa and Arab States*[111] held in Tunis, Tunisia in June 2009 (attended by ITIDA) serves to highlight some of the main challenges faced by countries in the region in enhancing cybersecurity and securing critical information infrastructures. Importantly, it focused on the way forward for countries to strengthen their cybersecurity frameworks.[112]

b. The African Union

It is worth noting that the African Union's (AU)[113] March 2008 *Study on Harmonisation* [sic] *of Telecommunication, Information and Communication Technologies Policies and Regulation in Africa*[114]

107. *See* LEAGUE OF ARAB STATES, http://www.arableagueonline.org (last visited Mar. 13, 2011) (English website under construction).

108. *See* United Nations Econ. & Soc. Comm'n for W. Asia, *Issues and Recommendations Related to Building Trust and Confidence in Online E-Services in the ESCWA Region* 22 (2010) ("The Tunisian Cyber Security Legal Framework.").

109. *See News Archive*, CYBERCRIME LAW, http://www.cybercrimelaw.net /Archive.html (scroll down to "2006 October") (last visited Mar. 13, 2011) ("Saudi Arabia has passed laws covering cybercrime. The Shoura Council has in October enacted provisions on illegal access, data interference, etc.").

110. *See The Prevention of Information Technology Crimes*, UNITED ARAB EMIRATES COMPUTER EMERGENCY RESPONSE TEAM (2006), http://www.aecert.ae /Prevention_of_Information_Technology_Crimes_English.pdf.

111. *See 2009 ITU Regional Cybersecurity Forum for Africa and Arab States*, INT'L TELECOMMS. UNION, http://www.itu.int/ITU-D/cyb/events/2009/tunis/index.html (last visited Mar. 15, 2011).

112. *See* ITU Regional Cybersecurity Forum 2009, *Draft Meeting Report*, Doc. No. RFT/2009/01-E, June 8, 2009, *available at* http://www.itu.int/ITU-D/cyb/events /2009/tunis/docs/tunis-cybersecurity-forum-report-june-09.pdf.

113. AFRICAN UNION, http://www.africa-union.org (last visited Feb. 11, 2011).

114. *See* AFRICAN UNION, STUDY ON HARMONISATION OF TELECOMMUNICATION, INFORMATION AND COMMUNICATION TECHNOLOGIES POLICIES AND REGULATION IN

identified the need for member countries to combat cybercrimes. Many African countries have taken the initiative and forged ahead with legislation to address cybercrime and data protection.

D. Institutional

The institutional arrangements supporting cybersecurity are as varied and diverse as the approaches to the issues. Two points merit noting at the outset. First, there is no one-size-fits-all response to effective institutional design. As will be demonstrated, institutional arrangements vary dramatically. Second, as was mentioned in Section II, not all cybersecurity issues have a specific institutional dimension. The most obvious one is the area of cybercrime, where practice indicates that issues of cybercrime, once passed into legislation, are usually within the purview of the police and the courts.

Briefly, there are the substantive areas that do lend themselves to special institutional arrangements, especially CIIP (usually through CERTs) and data privacy protection (here practice is highly divergent).

CERTs, described in section III.A.1, are one of the main responses to protecting infrastructure.[115] In some countries (ArCERT in Argentina,[116] the Canadian Cyber Incident Response Center (CCIRC),[117] MyCERT in Malaysia,[118] SingCERT in Singapore,[119] the Electronic Communications Security–Computer Security Incident Response Team in South Africa (ECS-CSIRT),[120] and tunCERT in Tunisia[121]), CERTs take on a formal institutional

AFRICA: EXECUTIVE SUMMARY (2008), *available at* http://www.africa-union.org/root/UA/conferences/2008/mai/ie/11-14mai/executivesummary%20study%20on%20telecom%20policy%2031%20mars.pdf.

115. For an alphabetical list of CERTS, see *First Members*, FIRST, http://www.first.org/members/teams/ (last visited Feb. 28, 2011).

116. *ArCERT*, FIRST, http://www.first.org/members/teams/arcert/ (last visited Mar. 13, 2011).

117. *CCIRC*, FIRST, http://www.first.org/members/teams/ccirc/ (last visited Feb. 28, 2011).

118. *MyCERT*, FIRST, http://www.first.org/members/teams/mycert/ (last visited Feb. 28, 2011).

119. *SingCERT*, FIRST, http://www.first.org/members/teams/singcert/ (last visited Feb. 28, 2011).

120. *ECS-CSIRT*, FIRST, http://www.first.org/members/teams/ecs-csirt/ (last visited Feb. 28, 2011).

121. *tunCERT*, FIRST, http://www.first.org/members/teams/tuncert/ (last visited Feb. 28, 2011).

role. These national CERTs also have various institutional reporting roles. ArCERT reports to the President through the National Office for IT. In Canada, CCIRC reports to the Prime Minister. MyCERT reports to the Prime Minister through the Ministry of Science. SingCERT reports to the Ministry of Information through the Infocomm Development Authority of Singapore (IDA). ECS-CERT I in South Africa reports to the President through the Minister of Data Secretary. tunCERT reports to the Ministry of Communications Technologies through the National Agency for Computer Security.

In terms of privacy, a number of examples demonstrate the wide practice of institutional responses:

- ***Argentina***. In Argentina, the National Data Protection Directorate (NDPD) established under the Personal Data Protection Act is responsible for digital data protection.[122] The NDPD is under the Ministry of Justice and Human Rights.
- ***Canada***. In Canada, at the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) assigns its oversight and enforcement role to the Office of the Privacy Commissioner of Canada (OPC) which reports to Parliament.
- ***European Union***. In the E.U., generally, each country has a Data Protection Agency (DPA) principally responsible for the interpretation and enforcement of data privacy violations. Each DPA is typically an independent agency, with the authority to enforce against other government entities. For those E.U. member states with a criminal component to data protection legislation, national or regional prosecutors may be engaged by the DPA for particular matters. In addition, at the E.U. level, there is a Working Party on Data Protection that determines which countries are compliant with the Directives.
- ***Malaysia***. In Malaysia, processing of personal data is regulated by the Personal Data Protection Act 2009 (PDPA). The Personal Data Protection Commissioner is appointed by the Ministry of Information, Culture, and Communications and is in charge of implementing and enforcing the personal data protection laws in Malaysia.

122. *Argentina Personal Data Protection Act (2000)*, PRIVACY INTERNATIONAL (Oct. 30, 2000), http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61939 (providing an English translation of the Argentina Personal Data Protection Act (2000)).

- ***Singapore***. Singapore is an interesting case. There is no overarching data protection or privacy law in Singapore. However, there are several industry-specific laws that deal with data protection and privacy issues and that may be enforced by industry regulatory bodies. In addition, while the Constitution of Singapore does not contain any explicit right to privacy, the High Court has ruled that personal information may be protected under a duty of confidence. Nevertheless, the government of Singapore has been considering passing a comprehensive data protection act for more than ten years now.[123]
- ***South Africa***. In South Africa, the Protection of Personal Information Act (PPIA) requires that personal information may only be processed by a responsible party that has notified the information Protection Regulator (Regulator), which reports to the President of South Africa.
- ***Tunisia***. In Tunisia, the Act on Protection of Personal Data established the National Authority for Protection of Personal Data (NAPPD). The NAPPD reports to the Ministry of Human Rights.

IV. INTERNATIONAL, NATIONAL, AND ORGANIZATIONAL RESPONSES[124]

A. *Promoting International Cooperation on Cybersecurity*

No nation-state can achieve adequate cybersecurity on its own; international coordination and cooperation must be part of the response.

Some believe that an international treaty is needed on some or all aspects of the cybersecurity problem. And in many cases, this clarion call relates to issues of "cyber-war" and arises in a number of *fora*.[125] As noted above, NATO issued an experts' report, "NATO

123. *PHR2006—Republic of Singapore*, PRIVACY INTERNATIONAL (Dec. 18, 2007), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559494 (displaying Privacy International's 2007 report on Singapore).

124. Having undertaken a brief substantive review of the themes and responsible institutions/organizations, this section provides a brief glimpse into some current responses to these issues.

125. In January 2010, Hamadoun Toure, former ITU Secretary General, proposed at the World Economic Forum in Davos that the world's nations should

2020: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO," which included recommendations for changes in the NATO Strategic Concept to specify the characteristics of a cyber attack that would trigger the obligation of collective response under Section 5 of the NATO treaty.[126] The report contains the following blunt statements:

> NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence [sic] capabilities aimed at effective detection and deterrence.
>
> . . . .
>
> The most probable threats to Allies in the coming decade are unconventional. Three in particular stand out: 1) an attack by ballistic missile (whether or not nuclear-armed); 2) strikes by international terrorist groups; and 3) cyber assaults of varying degrees of severity. . . .
>
> . . . .
>
> The Alliance should consider giving the Secretary General or NATO military leaders certain pre-delegated authorities, based on agreed rules-of-engagement, to respond in an emergency situation such as a missile or cyber attack.
>
> . . . .
>
> The next significant attack on the Alliance may well come down a fibre [sic] optic cable. Already, cyber attacks against NATO systems occur frequently, but most often below the threshold of political concern. However, the risk of a large-scale attack on NATO's command and

adopt a treaty in which they would engage not to make the first cyber strike against another nation. The ensuing debate revealed a considerable lack of clarity over what cyber-war is and what responses are appropriate for nation states to exercise. The fundamental issue is how does the "law of war"—including such core issues as necessity and proportionality and the very definition of "war" itself—apply to cyberspace. For example, assuming that use of force was otherwise justified, when would it be appropriate to attack the systems (SCADA) that control electrical and power infrastructure, and would it be necessary or even possible to distinguish between military (combatant) targets and civilian (non-combatant) targets? What would be the implications and what would be the proper range of responses if one nation state were to distribute against another the Stuxnet virus, which attacks SCADA systems? What issues surround use by a nation state of non-governmental proxies, such as bot-net operators, to conduct cyber-attacks?

126. NATO 2020: ASSURED SECURITY; DYNAMIC ENGAGEMENT, *supra* note 3, at 9.

> control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence [sic] measures under Article 5. . . . [T]here persist serious gaps in NATO's cyber defence [sic] capabilities. The Strategic Concept should place a high priority on addressing these vulnerabilities, which are both unacceptable and increasingly dangerous.[127]

Article 51 of the U.N. Charter provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence [sic] if an armed attack occurs against a Member of the United Nations. . . ."[128] The application of Article 51 with respect to cyber-war has been hotly debated in the academic literature without any firm conclusions being drawn.[129]

When analyzing the merits of a treaty-based approach to cybersecurity, a myriad of questions arise, including: What are the key issues that should or could be addressed in a cybersecurity treaty? What would be the added value of such a treaty? What would be the risks? What prior efforts have been attempted and what caused them to fail or have limited effect? What incremental steps can be taken to break through the problems? How can treaty compliance be verified? How could countries globally be supported in the strengthening of their cybersecurity capacities, through technical assistance and other means?

Any effort to reach international consensus on cybersecurity is likely to expose a range of concerns, which in part flow from different visions of national security, of the role and value of the

127. *Id.* at 11, 17, 35, 45.

128. U.N. Charter art. 51, *available at* http://www.un.org/en/documents/charter/chapter7.shtml.

129. *See* Jon P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275 (2008) (discussing the merits of a realist view of customary international law formation as a means of coping with the potential harms associated with modern information operations); Glen R. Shilland, Influencing and Exploiting Behavioral Norms in Cyberspace to Promote Ethical and Moral Conduct of Cyberwarfare (June 2010) (unpublished Master's thesis, Air University), *available at* https://www.afresearch.org/skins/RIMS/home.aspx (enter article title in search window and follow hyperlink to source) (exploring the interaction of the law of armed conflict with cyberspace behavioral norms and suggesting avenues to influence these norms in order to facilitate ethical and moral cyberwarfare); Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World*, 18 TRANSNAT'L L. & CONTEMP. PROBS. 657 (2009), http://www.uiowa.edu/~tlcp/TLCP%20Articles/18-3/stevens.finalfinal.me.mlb.100109.pdf (arguing that international law is insufficient to address cyber attacks).

Internet, of human rights, and of economic policy. Some see cybersecurity as having state security at its core, which leads to an emphasis on capabilities to monitor and attribute transmissions and to block any undesirable content. Others strongly believe that Internet governance (including Internet security) involves the integrating and balancing of interests, including not only national security, but also human rights and the economic and developmental interests associated with a vibrant, innovative, and competitive ICT sector. These differing perspectives manifest themselves in many areas, including, for example, the increasing debate over the issue of "attribution," referred to above. One contribution to reconciling these interests is the 2009 recommendation of the European Parliament on strengthening security and fundamental freedoms on the Internet.[130]

Various proposals are emerging for improving regional and international cooperation, including the following:

- The Council of Europe has started work to explore the shared responsibilities of states to take reasonable measures through multi-lateral cooperation "to ensure the ongoing functioning of the Internet and, in consequence, of the delivery of the public service . . . to which all persons under their jurisdiction are entitled."[131] In this connection, the competent intergovernmental cooperation body, the CoE Steering Committee on the Media and New Communication Services (CDMC), has been asked by the CoE Committee of Ministers to give priority attention to the elaboration of legal instruments designed (i) to preserve or reinforce the protection of the cross-border flow of Internet traffic and (ii) to protect resources which are critical for the ongoing functioning and borderless nature and integrity of the Internet (i.e. critical Internet resources).
- It was reported recently that Korea is attempting to present computer security as a topic of discussion for the Group of 20 meetings in Seoul later this year. Korea reportedly wants to

130. Strengthening Security and Fundamental Freedoms on the Internet, EUR. PARL. DOC. INI/2008/2160 (2009), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//EN.

131. 1st Council of Europe Conference of Ministers Responsible for Media and New Communication Services, *Resolution: Internet Governance and Critical Internet Resources*, *in* A NEW NOTION OF MEDIA? 9, 10 (May 28, 2009), *available at* http://www.coe.int/t/dghl/standardsetting/media/MCM%282009%29011_en_final_web.pdf.

include on the summit agenda discussion of establishing an international body for combating cybercrime.[132]

- In March 2009, the E.U. Commission issued a communication on Critical Information Infrastructure Protection (CIIP), entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience."[133] It noted that the challenges for Europe are: (1) uneven and uncoordinated national approaches; (2) need for a new European governance model for Critical Information Infrastructures; (3) limited European early warning and incident response capability; and (4) need for appropriate international cooperation. With respect to international cooperation, the communication spoke of "engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations [sic]." [134]
- In April 2009, the E.U. held a Ministerial Conference on CIIP.[135]
- The Organization of American States has undertaken a number of steps to enhance cybersecurity and improve regional responses to cybercrime.[136]
- One structure in Europe for improving coordination is the European Network and Information Security Agency (ENISA), founded in 2004.[137] ENISA planned the first pan-European CIIP exercise that took place in November 2010. The exercise

132. *See* Kim Tong-hyung, *Korea Trying to Put Cyber Security on G20 Agenda*, THE KOREA TIMES, Aug. 5, 2010, http://www.koreatimes.co.kr/www/news/biz/2010/11/123_70876.html.

133. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from Large Scale Cyber-Attacks and Disruptions Enhancing Preparedness, Security, and Resilience,"* at 7, SEC (2009), *available at* http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf.

134. *Id.* at 7.

135. *See Valérie Andrianavaly, EU Policy on Critical Information Infrastructure Protection—CIIP* (June 19, 2009), *available at* http://sta.jrc.ec.europa.eu/pdf/scni/ExperimentalPlatforms/1-CIIP_INFSO_WS%2020090619.pdf.

136. *See Inter-American Cooperation Portal on Cyber-Crime*, ORGANIZATION OF AMERICAN STATES, http://www.oas.org/juridico/english/cyber.htm (last visited Mar. 13, 2011).

137. *About ENISA*, EUROPEAN NETWORK AND INFO. SEC. AGENCY, http://www.enisa.europa.eu/about-enisa (last visited Mar. 13, 2011).

tested the efficiency of communication between different Member States in case of incidents affecting Internet's normal operation in all participating countries.

- Recently a group of governmental experts from fifteen countries agreed on a set of recommendations on cybersecurity.[138]

All of these recent examples raise important questions, including: What are the best venues for improving international cooperation? What is the role of intergovernmental organizations, such as the ITU, UNCITRAL, or the U.N. itself? What is the role of regional organizations, such as the African Union, APEC, the Council of Europe, the E.U., NATO, or the OAS? What is the role of the international business community and civil society globally? What incremental steps can be taken to advance cooperation?

B. Structuring National Responses

While international cooperation is necessary, each nation will have to develop, as a foundation, its own national cybersecurity strategy, authorities, and capabilities. Within any given nation state, adequate cybersecurity will require effective coordination and cooperation among governmental entities on the national and sub-national levels as well as the private sector and civil society.

Issues for consideration include: What are the most effective means to promote effective coordination and cooperation at the national level? To what extent should cooperation of the private sector be legally compelled? What incentives or subsidies may promote cooperation? How far should governments go in regulating the private sector in the name of improving cybersecurity? What is the role of civil liability systems in addressing cyber-vulnerabilities?

As governments seek to develop their own national policies and structures for cybersecurity, questions include: Which agency or ministry should have the lead? What should be the role of civilian agencies versus national security agencies? What should be the roles of law enforcement or national security agencies versus the roles of ministries for trade, commerce, or communications?

138. *See* John Markoff, *Step Taken to End Impasse Over Cypersecurity Talks*, N.Y. TIMES, July 16, 2010, at A7, http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1.

One example of a national strategy for cybersecurity is the Comprehensive National Cybersecurity Initiative (CNCI) developed by the U.S.[139] It is important to note that most elements of the U.S. plan focus on getting the federal government's own cybersecurity house in order. The U.S. has not decided what should be the regulatory authority of the federal government in protecting critical infrastructures owned and operated by the private sector. Pending legislation may clarify that role later this year. Another example is the European Programme for Critical Infrastructure Protection set forth in the "EU COM (2006) 786" directive, which obligates all member states to adopt the components of the Programme into their national statutes. The Programme also applied to the European Economic Area.[140]

One element of almost any cybersecurity strategy at the governmental or corporate level is the development and deployment of intrusion detection systems that monitor a given network for unauthorized traffic and malicious content. Key issues include whether an intrusion detection system for governmental networks should be extended to privately owned networks or whether the private sector should manage its own intrusion detection systems. If the answer in a particular nation is that an intrusion detection system for governmental networks should be extended to at least some more critical privately owned networks, the next question is on what principles is that category delineated. This issue also often leads to consideration of the role of national security or military agencies versus civilian agencies.

V. RECOMMENDATIONS FOR A WAY FORWARD

Having set the stage in Sections I and II, providing an overview of substantive issues of cybersecurity in Section III, and briefly outlining some international and national responses in Section IV, this Section proposes some additional thoughts for advancing the evolution of the international legal enabling environment for cybersecurity.

139. *Comprehensive National Cybersecurity Initiative*, *supra* note 36.

140. *See Communication from the Commission: On a European Programme for Critical Infrastructure Protection*, COM (2006) 786 final (Dec. 12, 2006), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

It is recognized, of course, that there are existing mechanisms and instruments of international cooperation on legal issues of cybersecurity among which the Council of Europe's Budapest Convention is primary. In this article, the authors suggest three main ideas towards an evolving international best practice legal approach to cybersecurity: First, an approach that deconstructs matters of cybersecurity. Second, an approach that looks at issues of cybersecurity in a modular way. And third, that these deconstructionist and modular approaches provide a new lens through which to look at how to enhance future international cooperation and collaboration.

Part of the deconstruction and modular approach advocated here is aimed at clarifying what exactly is meant by use of the catch-all phrase, "cybersecurity." Cybersecurity does not necessarily mean cybercrime, which does not necessarily mean cyber-war. Threats to cybersecurity come from a number of sources, including outdated legal architecture that doesn't necessarily reflect or apply well to the Internet and a dissonance of policy and legislative approaches by countries that make international collaboration and cooperation on certain levels difficult. In addition, "buggy code," bad practice, and simple human error, as well as natural disasters can thwart such efforts and contribute to cyber-insecurity.

So, going forward, what can be done to approach these new issues of cooperation? First, it is suggested that policy-makers and legislators adopt at the same time a more modular and a layered approach to the many complex and often intertwined questions of cybersecurity. Deconstruction begins by recognizing the manifold layers affected and tailoring security approaches to each layer. Those layers could include the infrastructure layer, the protocol or software layer, and the applications layer. In addition, a more resilience-based approach is emerging as the bellwether approach instead of a "perimeter" security approach. Finally, a better and more realistic understanding of the incentives of the different actors involved is required, including economic and personal incentives. Institutionally, attention needs to be paid to building capacity, especially for law enforcement personnel and by harnessing the expertise of the private sector and other industry players at the various levels through engagement with the private sector, possibly through innovative public-private partnership mechanisms.

In analyzing and addressing the complex, multidimensional tapestry of international cybersecurity legal issues, the following is a synthesis of factors to be taken into consideration[141]:

- *Deconstructionalist (layered) approach.* Cybersecurity is not a monolith and responses to cyber-threats do not come in a "one-size-fits-all" package. Rather, the analysis of threats to cybersecurity, as well as the responses to them, needs to be looked at both in a deconstructed and modular fashion.
- *Resilience vs. perimeter security.* Concepts of security based on "securing the perimeter" applicable in past decades to closed systems should be reviewed in favor of concepts of security based on resilience (flexibility of response to type of threat and ability to recover and adjust more quickly to changing threat environments).
- *Identify incentives.* A range of incentives (including economic and behavioral incentives) exist that should be (1) understood and (2) employed in the design of security response systems. This could even include identifying innovative incentives to change behavior of users, such as an insurance market that could accurately price the risk of security.
- *Fully implement existing instruments.* Many tools, instruments, and good practices are already available to help societies cope with cybercrime, including the Budapest Convention, but these need to be fully implemented and applied.
- *Increase awareness and build capacity.* These are especially needed in the case of policy-makers, legislators, regulators, and law enforcement personnel.
- *Ensure cybersecurity needs are adequately resourced.* (See above).
- *Create cybersecurity accountability.* In some countries, an accountable cybersecurity "czar" is named, but in others, or in systems with diffuse accountability, lack of clear identification of responsibility can lead to vulnerability.
- *Law reform.* Here, there are three areas meriting attention: First, in developing countries, a robust, comprehensive law reform component should be included in development projects. Second, national laws should be drafted with a view towards achieving, if not harmonization, interoperability

141. This list of factors is derived from the discussion of the panelists at the Workshop. For details of the discussion that gave rise to this synthetic list, see, for example, Transcript, *supra* note 10.

across borders. And third, international law responses can provide for improvements of the functioning, stability, and resilience of the Internet.

- *Sovereignty issues may require re-examining existing concepts of the "State."*
- *Use of PPP models and approaches.* Recognizing that no country or entity can address cybersecurity alone, governments should be encouraged to work with industry and civil society in addressing cybersecurity needs. Indeed, the private sector, since it owns much of the infrastructure and since it has resources and incentives for security, should be actively engaged, perhaps through a variety of public-private partnership models.

VI. SELECTED BIBLIOGRAPHIC REFERENCES

ACCESS DENIED—THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert, John Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2008).

AFRICAN UNION, STUDY ON HARMONISATION OF TELECOMMUNICATION, INFORMATION AND COMMUNICATION TECHNOLOGIES POLICIES AND REGULATION IN AFRICA: EXECUTIVE SUMMARY (2008), http://www.africa-union.org/root/UA/conferences/2008/mai/ie/11-14mai/executivesummary%20study%20on%20telecom%20policy%2031%20mars.pdf.

Alan Charles Raul & Ed McNicholas, *Defendant Prevails in Privacy Case Where Data Theft Results in No Injury to Plaintiffs*, PRIVACY & DATA SEC. L.J. (Oct. 2007), http://www.sidley.com/files/Publication/78c71ce8-e0f7-4759-8c13-44eb436d6e2e/Presentation/PublicationAttachment/ae6774ca-19de-4dd5-8282-464e81c50574/Randolph.pdf.

Alan Charles Raul & Edward McNicholas, *Federal Court of Appeals Dismisses Data Breach Class Action Following Hack of Bank's Marketing Web Site*, PRIVACY & DATA SEC. L.J. (Oct. 2007), http://www.sidley.com/files/Publication/30a0e526-942b-4b12-9f17-3ed0abeafa47/Presentation/PublicationAttachment/afb040ec-8c15-4572-a2c2-3f7ccf890411/Pisciotta.pdf.

Alan Charles Raul & Edward McNicholas, *French CNIL Examines Data Protection Issues Linked to U.S. Litigation Disclosures*, PRIVACY & DATA SEC. L.J. (Apr. 2008), http://www.sidley.com/files/Publication/5205b05c-4d8c-4c81-a717-9000e575bf98/Presentation/PublicationAttachment/853407a1-48e3-4ccc-98c1-91f1844ee474/French%20CNIL%20Examines%20Data%20Protection%20Issues%20Linked%20To%20U.S.%20Litigation%20Disclosures.pdf.

Alan Charles Raul, Edward McNicholas & Colleen Theresa Rutledge, *New State Attempts at Data Security Laws Offer Uncertain Promise,* PRIVACY & SEC. L. REP. (Jan. 7, 2008), http://www.sidley.com/files/Publication/faae4dfa-5c0d-439d-94ac-359e487f08b9/Presentation/PublicationAttachment/ebb9c167-0048-40fc-8419-3619dcdf8708/NewStateAttempts3.pdf.

Alan Charles Raul, Edward McNicholas & Jennifer Tatel, *Damages for the Harm of Data Breaches and Other Privacy Claims*, PRIVACY & SEC. L. REP. (Sept. 15, 2008), http://www.sidley.com /files/Publication/a63e7e29-6790-4148-9d6d-64ad5fc97e5c/Presentation /PublicationAttachment/35f59659-909b-4040-a719-6614948828bc /DamagesBNA.pdf.

Alan Charles Raul, Edward R. McNicholas, John M. Casanova, William R.M. Long & Julie M. Dwyer, *International Information Security: A Brief Survey of Global Data Security Regimes*, PRIVACY & SEC. L. REP. (June 26, 2006), https://www.privacyassociation.org /assets/presentations/07Summit/Remote_Info_Security_Security _Article_Summit07_Handout.pdf.

CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC, FACULTY OF LAW, UNIV. OF OTTAWA, APPROACHES TO SECURITY BREACH NOTIFICATION: A WHITE PAPER (2007), http://www.cippic.ca /documents/bulletins/BreachNotification_9jan07-print.pdf.

CHAIRMAN'S SUMMARY, INTERNET GOVERNANCE FORUM, THIRD MEETING OF THE INTERNET GOVERNANCE FORUM (IGF) (2008), http://www.intgovforum.org/cms/hydera/Chairman%27s %20Summary.10.12.2.pdf.

Chris Alberts, Audrey Dorofee, Georgia Killcrece, Robin Ruefle & Mark Zajicek, *Defining Incident Management Processes for CSIRTs: A Work in Progress* (2004), http://www.cert.org/csirts /resources.html (follow "Defining Incident Management Processes for CSIRTs: A Work in Progress" hyperlink).

Cisco Systems, Inc., *Data Leakage Worldwide: The High Cost of Insider Threats* (2008), http://www.cisco.com/en/US/solutions /collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf.

CLAY WILSON, CONG. RESEARCH SERV., COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS (2003), http://www.fas.org/irp/crs/RL32114.pdf.

COMMONWEALTH SECRETARIAT, MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME (2002), *available at* http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A Strategy for A Secure Information Society—"Dialogue, Partnership and Empowerment," COM (2006) 251 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF.

Council Directive 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:EN:PDF.

Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, E.T.S. No. 189, *available at* http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG.

Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG.

COUNCIL OF EUROPE, FACT SHEET 11: THE COUNCIL OF EUROPE AND CYBERCRIME (2009), https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=FS+11&Language=lanEnglish&Ver=original&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE.

COUNCIL OF EUROPE, GLOBAL PROJECT ON CYBERCRIME (PHASE 2): SUMMARY (2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/2079%20adm%20pro%20summary1a%20_20%20Feb%202009.pdf.

COUNCIL OF EUROPE, GUIDELINES FOR THE COOPERATION BETWEEN LAW ENFORCEMENT AND INTERNET SERVICE PROVIDERS AGAINST CYBERCRIME (2008), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

COUNCIL OF EUROPE, OCTOPUS INTERFACE CONFERENCE ON COOPERATION AGAINST CYBERCRIME, CONFERENCE CONCLUSIONS (2008), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_IF08-d-concl1c.pdf.

COUNCIL OF EUROPE, OCTOPUS INTERFACE CONFERENCE: COOPERATION AGAINST CYBERCRIME, PROGRAMME (2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/2079%20IF09-m-prog%20det%20pub5%20_6%20mar%2009_.pdf.

COUNCIL OF EUROPE, OCTOPUS INTERFACE CONFERENCE: COOPERATION AGAINST CYBERCRIME, QUESTIONNAIRE IN PREPARATION OF THE CONFERENCE (2007), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp (follow "Cybercrime legislation (questionnaire)" hyperlink under "Documents").

COUNCIL OF EUROPE, PROJECT ON CYBERCRIME: FINAL REPORT (2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567-d-final%20report1h%20provisional%20_14%20may%2009_%20+footnote.pdf.

COUNCIL OF EUROPE, PROJECT ON CYBERCRIME: PROGRESS REPORT (2008), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-3progrep1PROV-Public_11aug08_en.pdf.

CSIRT Services, CERT.ORG, http://www.cert.org/csirts/services.html (last updated Nov. 26, 2002).

EUROPEAN COMMISSION JUSTICE, PROTECTION OF PERSONAL DATA, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (last updated Apr. 8, 2011).

David Satola & W.J. Luddy Jr., *The Potential for an International Legal Approach to Critical Information Infrastructure Protection*, 47 JURIMETRICS J. 315–33 (2007), http://www.uncitral.org/pdf/english/colloquia/EC/Satola_LuddyArticleRev.pdf.

DEBIX INC., DATA BREACH INCIDENT RESPONSE WORKBOOK (2010), http://www.debix.com/workbook/index.php (click "Download the Data Breach Incident Response Workbook").

Deirdre Mulligan, *Spyware: The Latest Cyber-Regulatory Challenge*, TRANSCRIPT, Summer 2005, at 32, http://www.law.berkeley.edu/files/transcript_summer05.pdf.

Demi Getscko, Malcolm Harbour, Henry L. Judy, David Satola & Rajnesh Singh, *Global Best Practices—Consumer Protection and Data Breach Notification*, Presentation Made at the Internet Governance Forum—Rio de Janeiro, Brazil (Nov. 10, 2007), http://www.intgovforum.org/BPP2.php?went=27.

DOUG MARKIEWICZ, STATE SECURITY BREACH LEGISLATION (Vigilant Minds Inc. 2006), http://www.contrib.andrew.cmu.edu/~dmarkiew/docs/breach_whitepaper_200602.pdf.

ELGIN M. BRUNNER & MANUEL SUTER, INTERNATIONAL CIIP HANDBOOK 2008/2009 (Andreas Wenger et al. eds., 2008), *available at* http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=91952&lng=en.

EUROPEAN COMM. ON CRIME PROBLEMS (CDPC), COMM. OF EXPERTS ON THE OPERATION OF EUROPEAN CONVENTIONS ON CO-OPERATION IN CRIMINAL MATTERS (PC-OC), REPLIES ON MUTUAL LEGAL ASSISTANCE IN COMPUTER-RELATED CASES (Feb. 23, 2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/PC-OC%20_2008_%2008%20Rev%20add%20Computer%20Related%20cases.pdf.

EUROPEAN COMM. ON CRIME PROBLEMS (CDPC), COMM. OF EXPERTS ON THE OPERATION OF EUROPEAN CONVENTIONS ON CO-OPERATION IN CRIMINAL MATTERS (PC-OC), REPLIES ON MUTUAL LEGAL ASSISTANCE IN COMPUTER-RELATED CASES, ADDENDUM (2008), http://www.coe.int/t/dghl/cooperation/economiccrime

/cybercrime/T-CY/PC-OC%20_2008_%2008%20Rev%20Computer%20Related%20cases.pdf.

Evgeny Morozov, *Battling the Cyber Warmongers*, WALL ST. J., May 8, 2010, at W3, http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704370704575228653351323986.html.

Florian Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, THE CENTRE FOR EUROPEAN POLICY STUDIES (May 6, 2008), http://www.ceps.eu/book/taking-stock-databases-and-systems-information-exchange-area-freedom-security-and-justice.

GEORGE SADOWSKY ET AL., THE WORLD BANK, INFORMATION TECHNOLOGY SECURITY HANDBOOK (2003), *available at* http://www.infodev.org/en/Publication.18.html.

GEORGIA KILLCRECE, STEPS FOR CREATING NATIONAL CSIRTS (2004), *available at* http://www.cert.org/csirts/resources.html (Link available under "Creating a CSIRT: Getting Started").

GEORGIA KILLCRECE, KLAUS-PETER KOSSAKOWSKI, ROBIN RUEFLE & MARK ZAJICEK, ORGANIZATIONAL MODELS FOR COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTS) (2003), *available at* http://www.cert.org/csirts/resources.html (Link available under "Creating a CSIRT: Getting Started").

GEORGIA KILLCRECE, KLAUS-PETER KOSSAKOWSKI, ROBIN RUEFLE & MARK ZAJICEK, STATE OF THE PRACTICE OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs) (2003), *available at* http://www.cert.org/csirts/resources.html (Link available under "Operating Your CSIRT").

INT'L TELECOMM. UNION, CYBERSECURITY GUIDE FOR DEVELOPING COUNTRIES (2007), *available at* http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf.

JAMES R. LANGEVIN, MICHAEL T. MCCAUL, SCOTT CHARNEY & HARRY RADUEGE, CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace

_44.pdf.

J.H. Reichman & Paul F. Uhlir, *Database Protection at the Crossroads: Recent Developments and Their Impact on Science and Technology*, 14 BERKELEY TECH. L.J. 793 (1999), http://www.law.berkeley.edu/journals/btlj/articles/vol14/Reichman/html/reader.html.

JOHN MOTEFF, CONG. RESEARCH SERV., COMPUTER SECURITY: A SUMMARY OF SELECTED FEDERAL LAWS, EXECUTIVE ORDERS, AND PRESIDENTIAL DIRECTIVES (2004), http://www.fas.org/irp/crs/RL32357.pdf.

Joseph Turrow et al., *The FTC and Consumer Privacy in the Coming Decade*, FED. TRADE COMM'N (2006), http://works.bepress.com/cgi/viewcontent.cgi?article=1011&context=joseph_turow.

Julie E. Cohen, *DRM and Privacy,* 18 BERKELEY TECH. L.J. 575 (2003).

Lawrence A. Gordon, Martin P. Loeb, William Luchyshyn & Robert Richardson, *2006 CSI/FBI Computer Crime and Security Survey*, COMPUTER SECURITY INST. (2006), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

LORENZO PICOTTI & IVAN SALVADORI, COUNCIL OF EUROPE, NATIONAL LEGISLATION IMPLEMENTING THE CONVENTION ON CYBERCRIME—COMPARATIVE ANALYSIS AND GOOD PRACTICES (2008), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study2-d-version8%20_28%20august%2008.pdf.

Membership Process at a Glance, FIRST, http://first.org/membership (last visited Feb. 26, 2011).

MICHELA MENTING YOELL, INT'L TELECOMM. UNION, RESEARCH ON LEGISLATION IN DATA PRIVACY, SECURITY AND THE PREVENTION OF CRIME (2006), *available at* http://www.itu.int/ITU-D/cyb/publications/2006/research-legislation.pdf.

MOIRA J. WEST-BROWN, DON STIKVOORT, KLAUS-PETER KOSSAKOWSKI, GEORGIA KILLCRECE, ROBIN RUEFLE, & MARK ZAJICEK, HANDBOOK FOR COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTS) (2003), http://www.cert.org/csirts/resources.html (Link available under "Operating Your CSIRT").

Office of the Press Sec'y, *President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review,* THE WHITE HOUSE (Feb. 9, 2009), http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview.

ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY (2002), *available at* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007).

PERKINS COIE LLP, SECURITY BREACH NOTIFICATION CHART, http://www.digestiblelaw.com/files/upload/securitybreach.pdf (last visited June 30, 2011).

PONEMON INSTITUTE, BENCHMARK STUDY OF EUROPEAN AND U.S. CORPORATE PRIVACY PRACTICES (2006), *available at* http://www.whitecase.com/files/Publication/1e7a69e0-49e9-478e-abc1-303e107c4dd7/Presentation/PublicationAttachment/4a78432a-bd1f-4363-ab82-32fab1729a1e/Benchmark_Study_Privacy_Practices_updated.pdf.

Ponemon Institute Study Shows Lack of Accountability, Resources at Root of U.S. Corporate Data Loss Problem, PR NEWSWIRE, Aug. 28, 2006, http://www.prnewswire.com/news-releases/ponemon-institute-study-shows-lack-of-accountability-resources-at-root-of-us-corporate-data-loss-problem-56261842.html.

PROJECT ON CYBERCRIME, CYBERCRIME LEGISLATION—COUNTRY PROFILE: UNITED STATES OF AMERICA (2007), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile-USAMarch08.pdf.

Ramona R. Rantala, *Cybercrime Against Businesses*, U.S. DEP'T OF JUST. BUREAU OF JUST. STAT. (Mar. 2004), http://bjs.ojp.usdoj.gov/content/pub/pdf/cb.pdf.

Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act,* 18 BERKELEY TECH. L.J. 909 (2003).

Resources for Computer Security Incident Response Teams (CSIRTs), CERT.ORG, http://www.cert.org/csirts/resources.html (last visited Mar. 5, 2011).

RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010).

Rob van den Hoven van Genderen, *Cybercrime Investigation and the Protection of Personal Data and Privacy*, COUNCIL OF EUROPE (2008), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study5-d-provisional.pdf.

ROBERT BRUCE ET AL., CYBER SECURITY: A NEW MODEL FOR PROTECTING THE NETWORK 8 (2006), http://www.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/CyberSecurity.pdf.

Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity*, COUNCIL ON FOREIGN RELATIONS, INT'L INSTITUTIONS AND GLOBAL GOVERNANCE PROGRAM, Council Special Report No. 56 (2010), *available at* http://irps.ucsd.edu/assets/001/501278.pdf.

RONALD W. DEL SESTO, JR. & JON FRANKEL, HOW DEEP PACKET INSPECTION CHANGED THE PRIVACY DEBATE (2008), http://www.bingham.com/Media.aspx?MediaId=7514.

Samuelson Law, *Security Breach Notification Laws: Views from Chief Security Officers*, TECH. & PUB. POLICY CLINIC UNIV. CAL., BERKELEY (Dec. 2007), http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf.

SCOTT CHARNEY, RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD (2009), http://www.microsoft.com /downloads/details.aspx?FamilyID=062754CC-BE0E-4BAB-A181-077447F66877&displaylang=en&displaylang=en (follow "Download" near "Rethinking the Cyber Threat—A Framework and Path Forward").

Secretary-General of the OECD, *The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries*, OECD (Dec. 16, 2005), http://www.oecd.org/dataoecd/16/27 /35884541.pdf.

STAFF OF H.R. COMM. ON GOVERNMENT REFORM, 109TH CONG., AGENCY DATA BREACHES SINCE JANUARY 1, 2003 (Oct. 13, 2006), http://www.govexec.com/pdfs/AgencyBreachSummaryFinal.doc.

Staffing Your Computer Security Incident Response Team, CERT.ORG, http://www.cert.org/csirts/csirt-staffing.html (last visited Mar. 5, 2011).

Stanley W. Crosley, Alan Charles Raul, Edward R. McNicholas & Julie M. Dwyer, *A Path to Resolving European Data Protection Concerns with U.S. Discovery*, 6 PRIVACY & SEC. L. REP. (2007), http://www.sidley.com /files/Publication/7ed26a68-1ec7-44eb-9db6-3660d938f575 /Presentation/PublicationAttachment/166eaabb-2a74-43fe-8a96 -3d78194ec198/EuroDataProtection.pdf.

STEIN SCHJOLBERG, INT'L TELECOMM. UNION, GLOBAL STRATEGIC REPORT (2008), *available at* http://www.itu.int/osg /csd/cybersecurity/gca/docs/global_strategic_report.pdf.

STEIN SCHJOLBERG, INT'L TELECOMM. UNION, REPORT OF THE CHAIRMAN OF HLEG (2008), *available at* http://www.itu.int/osg /csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG _to_ITU_SG_03_sept_08.pdf.

Stein Schjolberg, *Proposal for a Memorandum of Understanding (MoU),* THE GENEVA PROTOCOL ON CYBERSECURITY AND CYBERCRIME, http://www.cybercrimelaw.net/documents/Proposal _for_a_Geneva_Protocol.pdf.

Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation—The Road to Geneva*, CYBERCRIME LAW (Dec. 2008), http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.

STEIN SCHJOLBERG & AMANDA M. HUBBARD, INT'L TELECOMM. UNION, HARMONIZING NATIONAL LEGAL APPROACHES ON CYBERCRIME (2005), http://www.estig.ipbeja.pt/~ac_direito/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

Stephen Kinsella, Alan Charles Raul, Edward McNicholas & Hanne Melin, *Public Right of Access to Lobbyist Information Trumps EU Privacy Rights*, PRIVACY & DATA SEC. L. J., at 31 (Jan. 2008), http://www.sidley.com/files/Publication/5684ea72-5757-454b-9d68-4ab1ad16a3de/Presentation/PublicationAttachment/a1ae5b08-363e-46f3-89c0-4ac5e5e68af7/McNicholas%2003.10.08.pdf.

STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010).

SYNOVATE, FEDERAL TRADE COMMISSION—2006 IDENTITY THEFT SURVEY REPORT (2007), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

The Cybercrime Convention Comm., 3rd Multilateral Consultation of the Parties to the Convention on Cybercrime, Apr. 2008, E.T.S. No. 185, *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/T-CY%20_2008_%2004%20E%20-%20LONG%20REPORT%20FINAL.pdf.

The Cybercrime Convention Comm., Multilateral Consultation Among the Contracting States to the Convention on Cybercrime, Mar. 17, 2009, http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%205%20E.pdf.

THE E-GOVERNMENT HANDBOOK FOR DEVELOPING COUNTRIES, INFODEV (Nov. 2002), *available at* http://www.infodev.org/en/Publication.16.html.

Untangling Attribution: Moving to Accountability in Cyberspace: Hearing on Planning for the Future of Cyber Attack Before the H.

Subcommittee on Technology and Innovation, 111th Cong. (2010), (statement of Robert K. Knake, International Affairs Fellow in Residence, The Council on Foreign Relations), http://www.cfr.org/united-states/untangling-attribution-moving-accountability-cyberspace/p22630.

U.S. DEPT. HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (Feb. 2003), http://www.globalsecurity.org/security/library/policy/national/cyberspace_strategy2003.pdf.

WADE H. BAKER, C. DAVID HYLENDER & J. ANDREW VALENTINE, 2008 DATA BREACH INVESTIGATIONS REPORT: A STUDY CONDUCTED BY THE VERIZON BUSINESS RISK TEAM (2008), http://www.verizonbusiness.com/resources/security/databreachreport.pdf.